AlvariSTAR™

User Manual

SW Version 3.0
November 2006
P/N 214150

Document History

Topic	Description	Date Issued
Version 3.0 is regarded as the first publication of this manual.		November 2006

Legal Rights

© Copyright 2006 Alvarion Ltd. All rights reserved.

The material contained herein is proprietary, privileged, and confidential and owned by Alvarion or its third party licensors. No disclosure thereof shall be made to third parties without the express written permission of Alvarion Ltd.

Alvarion Ltd. reserves the right to alter the equipment specifications and descriptions in this publication without prior notice. No part of this publication shall be deemed to be part of any contract or warranty unless specifically incorporated by reference into such contract or warranty.

Trade Names

Alvarion®, BreezeCOM®, WALKair®, WALKnet®, BreezeNET®, BreezeACCESS®, BreezeMANAGE™, BreezeLINK®, BreezeCONFIG™, BreezeMAX™, AlvariSTAR™, AlvariCRAFT™, BreezeLITE™, MGW™, eMGW™, WAVEXpress™, MicroXpress™, WAVEXchange™, WAVEView™, GSM Network in a Box and TurboWAVE™ and/or other products and/or services referenced here in are either registered trademarks, trademarks or service marks of Alvarion Ltd.

All other names are or may be the trademarks of their respective owners.

Statement of Conditions

The information contained in this manual is subject to change without notice. Alvarion Ltd. shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or equipment supplied with it.

Warranties and Disclaimers

All Alvarion Ltd. ("Alvarion") products purchased from Alvarion or through any of Alvarion's authorized resellers are subject to the following warranty and product liability terms and conditions.

Exclusive Warranty

(a) Alvarion warrants that the Product hardware it supplies and the tangible media on which any software is installed, under normal use and conditions, will be free from significant defects in materials and workmanship for a period of fourteen (14) months from the date of shipment of a given Product to Purchaser (the "Warranty Period"). Alvarion will, at its sole option and as Purchaser's sole remedy, repair or replace any defective Product in accordance with Alvarion' standard R&R procedure.

(b) With respect to the Firmware, Alvarion warrants the correct functionality according to the attached documentation, for a period of fourteen (14) month from invoice date (the "Warranty Period")". During the Warranty Period, Alvarion may release to its Customers firmware updates, which include additional performance improvements and/or bug fixes, upon availability (the "Warranty"). Bug fixes, temporary patches and/or workarounds may be supplied as Firmware updates.

Additional hardware, if required, to install or use Firmware updates must be purchased by the Customer. Alvarion will be obligated to support solely the two (2) most recent Software major releases.

ALVARION SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY PURCHASER'S OR ANY THIRD PERSON'S MISUSE, NEGLIGENCE, IMPROPER INSTALLATION OR IMPROPER TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING OR OTHER HAZARD.

Disclaimer

(a) The Software is sold on an "AS IS" basis. Alvarion, its affiliates or its licensors MAKE NO WARRANTIES, WHATSOEVER, WHETHER EXPRESS OR IMPLIED, WITH RESPECT TO THE SOFTWARE AND THE ACCOMPANYING DOCUMENTATION. ALVARION SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT WITH RESPECT TO THE SOFTWARE. UNITS OF PRODUCT (INCLUDING ALL THE SOFTWARE) DELIVERED TO PURCHASER HEREUNDER ARE NOT FAULT-TOLERANT AND ARE NOT DESIGNED, MANUFACTURED OR INTENDED FOR USE OR RESALE IN APPLICATIONS WHERE THE FAILURE, MALFUNCTION OR INACCURACY OF PRODUCTS CARRIES A RISK OF DEATH OR BODILY INJURY OR SEVERE PHYSICAL OR ENVIRONMENTAL DAMAGE ("HIGH RISK ACTIVITIES"). HIGH RISK ACTIVITIES MAY INCLUDE, BUT ARE NOT LIMITED TO, USE AS PART OF ON-LINE CONTROL SYSTEMS IN HAZARDOUS ENVIRONMENTS REQUIRING FAIL-SAFE PERFORMANCE, SUCH AS IN THE OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR COMMUNICATION SYSTEMS, AIR TRAFFIC CONTROL, LIFE SUPPORT MACHINES, WEAPONS SYSTEMS OR OTHER APPLICATIONS REPRESENTING A SIMILAR DEGREE OF POTENTIAL HAZARD. ALVARION SPECIFICALLY DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY OF FITNESS FOR HIGH RISK ACTIVITIES.

(b) PURCHASER'S SOLE REMEDY FOR BREACH OF THE EXPRESS WARRANTIES ABOVE SHALL BE REPLACEMENT OR REFUND OF THE PURCHASE PRICE AS SPECIFIED ABOVE, AT ALVARION'S OPTION. TO THE

FULLEST EXTENT ALLOWED BY LAW, THE WARRANTIES AND REMEDIES SET FORTH IN THIS AGREEMENT ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING BUT NOT LIMITED TO WARRANTIES, TERMS OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, CORRESPONDENCE WITH DESCRIPTION, NON-INFRINGEMENT, AND ACCURACY OF INFORMATION GENERATED. ALL OF WHICH ARE EXPRESSLY DISCLAIMED. ALVARION' WARRANTIES HEREIN RUN ONLY TO PURCHASER, AND ARE NOT EXTENDED TO ANY THIRD PARTIES. ALVARION NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS.

Limitation of Liability

(a) ALVARION SHALL NOT BE LIABLE TO THE PURCHASER OR TO ANY THIRD PARTY, FOR ANY LOSS OF PROFITS, LOSS OF USE, INTERRUPTION OF BUSINESS OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES OF ANY KIND, WHETHER ARISING UNDER BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE AND WHETHER BASED ON THIS AGREEMENT OR OTHERWISE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

(b) TO THE EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE LIABILITY FOR DAMAGES HEREUNDER OF ALVARION OR ITS EMPLOYEES OR AGENTS EXCEED THE PURCHASE PRICE PAID FOR THE PRODUCT BY PURCHASER, NOR SHALL THE AGGREGATE LIABILITY FOR DAMAGES TO ALL PARTIES REGARDING ANY PRODUCT EXCEED THE PURCHASE PRICE PAID FOR THAT PRODUCT BY THAT PARTY (EXCEPT IN THE CASE OF A BREACH OF A PARTY'S CONFIDENTIALITY OBLIGATIONS).

Important Notice

This user manual is delivered subject to the following conditions and restrictions:

- This manual contains proprietary information belonging to Alvarion Ltd. Such information is supplied solely for the purpose of assisting properly authorized users of the respective Alvarion products.
- No part of its contents may be used for any other purpose, disclosed to any person or firm or reproduced by any means, electronic and mechanical, without the express prior written permission of Alvarion Ltd.
- The text and graphics are for the purpose of illustration and reference only. The specifications on which they are based are subject to change without notice.
- The software described in this document is furnished under a license. The software may be used or copied only in accordance with the terms of that license.
- Information in this document is subject to change without notice. Corporate and individual names and data used in examples herein are fictitious unless otherwise noted.
- Alvarion Ltd. reserves the right to alter the equipment specifications and descriptions in this publication without prior notice. No part of this publication shall be deemed to be part of any contract or warranty unless specifically incorporated by reference into such contract or warranty.
- The information contained herein is merely descriptive in nature, and does not constitute an offer for the sale of the product described herein.
- Any changes or modifications of equipment, including opening of the equipment not expressly approved by Alvarion Ltd. will void equipment warranty and any repair thereafter shall be charged for. It could also void the user's authority to operate the equipment.

About This Manual

The AlvariSTAR User Manual comprises the following chapters:

- Chapter 1 - Introduction - provides an overview of the AlvariSTAR system and its functionality.
- Chapter 2 - Permissions - describes how to define and manage user permissions and access rights for AlvariSTAR users.
- Chapter 3 - Inventory - describes how to access the AlvariSTAR functions for managing the system: Managed Network, Equipment Manager, Location Manager, Contact Manager, Backup Files Manager and PM Collection Viewer.
- Chapter 4 - Provisioning - describes the tools for viewing and managing Services and related entities (Subscribers and Service Profiles) in the entire network.
- Chapter 5 - System Utilities - describes the following system-wide utilities: Task Manager, License Manager, User Monitor and Audit Logs.
- Chapter 6 - Event Services - describes the tools for managing events generated in the system.

Contents

Chapter 1 - Introducing AlvariSTAR

1.1 About AlvariSTAR 2

1.2 AlvariSTAR Functionality 3

1.3 Starting the Application 6

1.3.1 Post Installation Checklist 6

1.3.2 Quick Start 7

1.3.3 Starting AlvariSTAR 9

1.3.4 Logging On 9

1.3.5 Logging Off 10

1.3.6 Change Password 11

1.3.7 Disabled Accounts 12

1.3.8 Application Server 13

1.4 The Home Window 14

1.5 The About Window 14

1.6 The Main Window 15

1.6.1 Main Menu 15

1.6.2 Toolbar 17

1.6.3 Navigation Pane 19

1.6.4 Work Area 22

1.6.5 Status Bar 23

1.7 Conventions and Common Operations 24

1.7.1 Conventions 24

1.7.2 Accelerators and Shortcuts 24

1.7.3 Control Buttons 24
1.7.4 Working with Tables 25
1.7.5 Manipulating the Displayed Information 26
1.8 How to Get Help 28

Chapter 2 - Permissions

2.1 Overview 30
2.2 User Manager 31
2.2.1 The User Manager Window 31
2.2.2 User Manager Controls 32
2.2.3 Adding or Modifying a User 33
2.3 User Group Manager 40
2.3.1 Adding or Modifying a Group 41
2.3.2 Deleting a Group 42
2.3.3 Default User Groups and Users 42
2.4 Functional Permissions 43
2.4.1 The Functional Permissions Page 43
2.4.2 Function Associations 45
2.4.3 Functional Permissions Editor 45
2.5 Application Security Policy 48
2.5.1 Login Policy 48
2.5.2 Password Policy 50
2.5.3 Password Constraint 52
2.6 Group Rights Summary 54

Chapter 3 - Inventory

3.1 Managed Network 56
3.1.1 Network IP Address Ranges Tab 56

3.1.2 Network Communities Tab 59

3.2 Equipment Manager 61

3.2.1 Filtering the List of Devices 64

3.2.2 The Equipment Editor 64

3.3 Location Manager 67

3.3.1 Searching for a Location 69

3.3.2 Location Editor 69

3.3.3 Coordinate Types 71

3.3.4 Location Map 71

3.4 Contact Manager 74

3.4.1 Associating Devices with a Contact 75

3.4.2 Creating or Modifying a Contact 75

3.5 Backup Files Manager 77

3.5.1 Restore Configuration Task 78

3.6 PM Collection Viewer 81

3.6.1 The Graph Generator 83

3.6.2 Exporting Collected Data 87

Chapter 4 - Provisioning

4.1 Introduction to Provisioning 90

4.2 Service Manager 91

4.3 Service Profile Manager 95

4.3.1 The Service Profile Manager Window 95

4.3.2 The Service Profile Editor 98

4.3.3 The Service Profile Distribution Task 108

4.4 Subscriber Manager 113

4.4.1 The Subscriber Manager Window 113

4.4.2 The Subscriber Editor 116

Chapter 5 - System Utilities

5.1 Introduction 126

5.2 Task Manager 127

5.2.1 Scheduling Tasks 130

5.2.2 The Task Results Viewer 133

5.2.3 Network Scan Task 134

5.2.4 Database Aging Task 135

5.2.5 BreezeMAX Service Profile Distribution Task 137

5.2.6 Single Range Scan Task 138

5.2.7 Performance Collection Task 140

5.2.8 BreezeMAX Software Upgrade Task 146

5.2.9 BreezeMAX Configuration Backup Task 154

5.3 License Manager 157

5.3.1 Adding Licenses 158

5.3.2 Activating Existing Licenses 158

5.4 User Monitor 159

5.5 Audit Logs 161

Chapter 6 - Event Services

6.1 Event Services 166

6.2 Event Monitor 167

6.3 Event History 170

6.4 Managing Alarms 172

6.4.1 Alarm Table 172

6.4.2 Alarm Severities 174

6.4.3 Alarm Details Window 175

6.4.4 Alarm Operations 179
6.4.5 Control Buttons 180
6.5 Event Template Manager 182
6.5.1 Creating Event Templates 183
6.5.2 Editing Event Templates 196
6.5.3 Deleting Event Templates 197
6.5.4 Importing Event Templates 197
6.6 Northbound Manager 198
6.6.1 Creating or Northbound System Definitions 199
6.6.2 General Page 201
6.6.3 Filters Page 202
6.6.4 Editing Northbound System Definitions 204
6.6.5 Deleting Northbound System Definitions 205
6.7 Event View Manager 206
6.7.1 Filtering Event Views 207
6.7.2 Default Event View 207
6.7.3 Creating Event Views 207
6.7.4 Editing Event Views 209
6.7.5 Deleting Event Views 210
6.8 Event Filter Manager 211
6.8.1 Filtering Event Filters 212
6.8.2 Default Event Filter 212
6.8.3 Managing Filter Criteria 212
6.8.4 Creating Event Filters 215
6.8.5 Editing Event Filters 216
6.8.6 Deleting Event Filters 217

6.8.7 Archiving Alarms 217

6.9 Command Manager 218

6.9.1 Creating Commands 219

6.9.2 Editing Commands 220

6.9.3 Deleting Commands 221

Index 223

1

Chapter 1 - Introducing AlvariSTAR

In This Chapter:

- "About AlvariSTAR" on page 2
- "AlvariSTAR Functionality" on page 3
- "Starting the Application" on page 6
- "The Home Window" on page 14
- "The About Window" on page 14
- "The Main Window" on page 15
- "Conventions and Common Operations" on page 24
- "How to Get Help" on page 28

1.1 About AlvariSTAR

AlvariSTAR is a comprehensive, Carrier-Class Network Management System (NMS) for Alvarion's Broadband Wireless Access products-based networks. AlvariSTAR is designed for today's most advanced service provider Network Operation Centers (NOCs), providing the network OA&M staff and managers with all the network surveillance, monitoring and configuration capabilities required in order to effectively manage the BWA network while keeping the resources and expenses at a minimum.

AlvariSTAR is designed to offer the network's OA&M staff with a unified, scalable and distributable Network Management System. AlvariSTAR uses a distributed client-server architecture, which provides the service provider with a robust, scalable and fully redundant Network Management System in which all single points of failure can be avoided.

1.2 AlvariSTAR Functionality

AlvariSTAR provides the following BWA network management functionality:

- Managed Network Application, allowing management of device discovery for identifying and adding existing devices to the managed devices database.
- Equipment Management, allowing viewing of devices in the database according to various search criteria, access to devices' dependent features, such as single and multiple device configuration managers and maps, access to the Configuration Backup Task for creating backup files for a selected device, and exporting of general information of selected devices to a Commas Separated Value (CSV) file.
- Single and Multiple Device Management, allowing comprehensive configuration and management of devices.
- Location Management, allowing definition and organization of hierarchical locations and associating them with maps and other attributes.
- Contact Management, allowing definition of contact persons and attributes to be associated with selected devices.
- Topology, providing Geographical hierarchical topology views for selected objects.
- Task Management, allowing definition and scheduling of system-wide background tasks, including:
  - Network scan, allowing to scan the network for new devices
  - Database Aging, allowing automation of database management tasks.
  - Service Profile Distribution, allowing deployment of Service Profiles in one or more Base Stations.
  - Single Range Scan, allowing to scan a predefined range of IPs for new and modified devices.
  - Performance Collection, allowing definition of criteria for on-going data collection sessions from managed devices/services.

- Software Upgrade, allowing efficient loading of new software versions to multiple devices simultaneously, and management of software versions in the devices.
- Configuration Backup, allowing backup of configuration of all or selected devices.

- Backup Files Management - enabling to restore, import, and export configuration backup files generated via the Configuration Backup task.
- Performance Monitring Viewer, allowing viewing graphs of selected counters that were collected using the Performance Monitoring Collection Task, and exporting collected data as CSV files.
- Audit Logs, allowing viewing of logged events.
- Event Monitoring, providing alerts and real-time updates of defined alarms.
- Event History Management, providing the ability to query the database for alarms in specific time intervals.
- Event Template Management, allowing customization and management of event templates according to specific preferences and needs.
- Northbound interface to other Network Management Systems.
- Security Management, allowing management of users, user groups, functional permissions and passwords.

Certain features are applicable only for certain product lines. These product line dependent features include:

- Subscriber Management, allowing creation and management of subscribers for service provisioning.
- Service Profile Management, allowing creation and management of service profiles incorporating various Quality of Service levels, priority based classifiers and forwarding rules.
- Service Management, allowing assignment of services to end users, including support of various user dependent features such as VLAN.

Embedded with the entire knowledge-base of BWA network operations, AlvariSTAR is a unique state-of-the-art power multiplier in the hands of the service provider that enables the provisioning of satisfied customers. AlvariSTAR dramatically extends the abilities of the service provider to provide a rich portfolio of services and to support rapid customer base expansion.

NOTE

This manual describes the general features of AlvariSTAR. To manage specific Alvarion product families, refer to the applicable Device Manager User Manual.

1.3 Starting the Application

AlvariSTAR enforces security at the client level. To log in to the application, you must have a valid user ID and password.

Before you can run this application your system must have running Application, and Database Servers. Typical installations implement the Application Server so it runs in the background, even after you log out of the client. See the Installation Manual for information about installing and configuring these required server processes (called *services* in Windows, *daemons* in Solaris).

1.3.1 Post Installation Checklist

Before starting the client application, verify the following:

1.3.1.1 License

The default demo license is valid for 60 days and is good for a limited number of devices (5 Base Stations, 5 Micro Base Stations, 100 SUs). To obtain a permanent license, contact your AlvariSTAR reseller. To load and activate a new license key, see "License Manager" - Section 5.3.

1.3.1.2 Device Configuration

To discover and manage devices, the AlvariSTAR Application Server that serves a given device must be defined in the device as an authorized manager, with the applicable SNMP parameters properly configured and with trap sending enabled.

CAUTION

For AlvariSTAR to function properly, the Admin Status of the Configuration Change trap should always be set to Enable. See the Traps Control Page in the Device Manager User Manual.

NOTE

In certain devices (such as BreezeMAX), if no Authorized Manager is defined in the device, it can be managed using SNMP with the default communities (private for read/write, public for read-only) by any station. If at least one Authorized Manager is defined, the device can be managed only by a station whose parameters match a defined Authorized Manager.

1.3.1.3 SW Upgrade Files

Software Upgrade files need to be stored on the Application Server in the AlvariSTAR firmware repository folder: <AlvariSTAR home>\filesystem\ firmware\rb.

NOTE

The “rb” folder should be manually created.
Use forward slashes in UNIX systems.

1.3.1.4 SNMP Ports

Verify that the SNMP ports (161, 162) are not used by any other application running on the computer. If Windows or any other SNMP Server is installed, open the Windows Service Manager, stop the SNMP Services and disable it to ensure that it will not start automatically the next time you restart the computer.

1.3.1.5 Security Enforcement

The Administrator should disable default users and define users, user groups, passwords and functional permissions (refer to Chapter 2).

1.3.2 Quick Start

The following is an overview that covers the basic steps for getting started with the AlvariSTAR management process. Refer to the respective chapter in this manual for an in-depth explanation of each step.

1. Define Data Aging Policies for database management tasks: Alarms and Audit Log records. (Refer to Section 5.2.4.)
2. Schedule the Data Aging task to automatically execute it. (Refer to Section 5.2.1.)
3. Customize the Event View and Event Filter to comply with your needs. (Refer to Section 6.2 and Section 6.3.)
4. Design the equipment location hierarchy. Define locations and sub-locations and associate them with maps if applicable. (Refer to Section 3.3.)
5. Define security policy and assign permissions to users/user groups. (Refer to Chapter 2.)
6. Open the Managed Network Application. Enter the necessary IP address ranges, locations and SNMP communities. Define all other applicable parameters and initiate discovery. (Refer to Section 3.1 for information on using the Managed Network application and Section 5.2.3 for information on running the Network Scan for equipment discovery.)
7. After devices are discovered and stored in the database, you can fully use the application to manage the system:

- Use the Equipment Manager to view devices in the database according to various search criteria. From the Equipment Manager you can access the devices' dependent Configuration and Multiple Configuration managers and geographical maps. (Refer to Section 3.2.)
- Use the Location Manager to design and manage hierarchical locations and associate them with maps. (Refer to Section 3.3.)
- Use the Contact Manager to define contact persons and attributes to be associated with selected devices. (Refer to Section 3.4.)
- Use the Performance Collection Task to define criteria for data collection from specified devices/services. (Refer to Section 5.2.7.)
- Use the Backup Files Manager to restore, import, and export configuration backup files generated via the Configuration Backup task.
- Use the PM Collection Viewer to display graphs of selected counters and export collected data as Comma Separated Values (csv) files. (Refer to Section 3.6.)
- Use the Software Upgrade Task to load software upgrade files and to manage SW versions in the devices. (Refer to Section 5.2.8.)
- Use the Provisioning options (if applicable to the managed device family) to define Subscribers, Service Profiles and Services and assign Services to subscribers. (Refer to Chapter 4 and to the Service Provisioning section in the User Guide of the relevant Device Manager.)
- Schedule tasks. (Refer to Section 5.2.1.)
- Use the Database Aging Task to control database management tasks including Alarms and Audit Log Records. (Refer to Section 5.2.4.)
- Use the License feature to view information on licensed vs. discovered devices, enabling you to estimate when you need to update your license. (Refer to Section 5.3.)
- Use the User Monitor feature to identify other currently active users and communicate with them. (Refer to Section 5.4.)
- Use the Audit Log Manager to view logged events. (Refer to Section 5.5.)
- Use the Event Monitor to view alarms and other events in real time. (Refer to Section 6.2.)
- Use the Event History to query the database for events and alarms in specific time intervals. (Refer to Section 6.3.)

- Use the Northbound Manager to interface with other Network Management Systems. (Refer to Section 6.6.)
- Use the Command Manager to create script commands that can be tiggered by template-matched alarms.

1.3.3 Starting AlvariSTAR

To start the application:

From the Windows Start menu, select *AlvariSTAR* > *Start Client Console*.

1.3.4 Logging On

To log in, type a valid user name and password at the login prompt, as follows:

Default User ID	Default Passwords
admin	admin
supervisor	supervisor
technician	technician
monitor	monitor

The application prompts you to change the password the first time it starts.

By default, you have three attempts to enter the correct password before the system aborts the login.

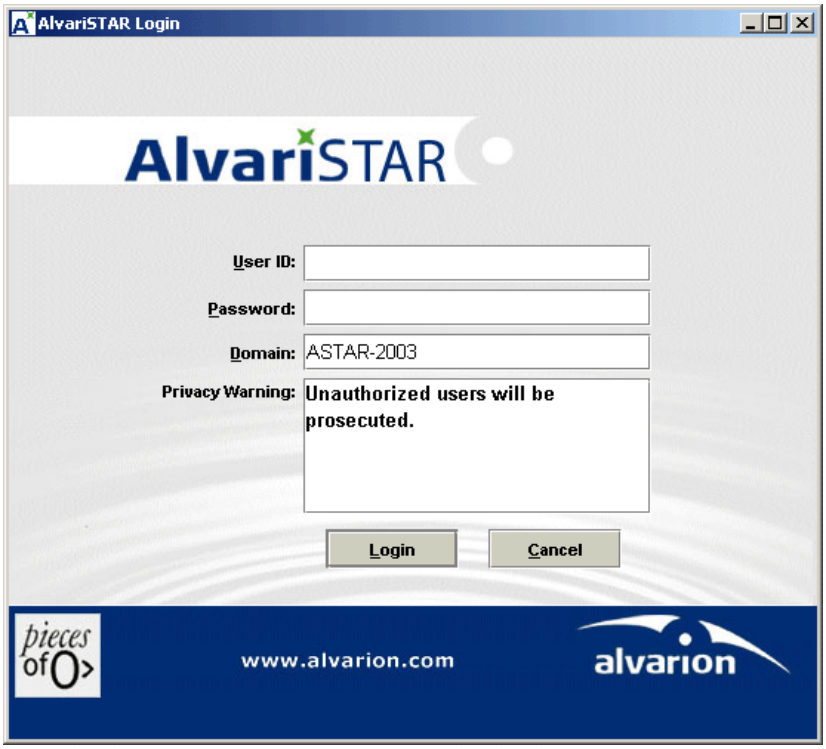

Figure 1-1: Login Prompt

1.3.5 Logging Off

The Exit feature shuts down the AlvariSTAR client application, while the Application Server continues to run. It is recommended to close all windows before exiting the client application.

To close windows:

From the *File* main menu, select **Close** to close the active window, or **Close All** to close all open windows.

To shut down AlvariSTAR client:

1. From the main menu select *File* > *Exit,* or, use the X icon displayed on the right upper corner of the main window, or use the *Ctrl+X* shortcut. A confirmation message is displayed.
2. Click **OK** to confirm.

1.3.6 Change Password

After initial login, the application prompts you to change the password. By default, there are no password constraints.

To change the password:

1. From the main menu, select *Settings* > *Change Password*. The Change Password dialog is displayed.
2. Enter the old password.
3. Enter the new password according to the password constraints displayed in the Change Password dialog. Confirm it.
4. Select *File* > *Save* (or use the *Ctrl+S* shortcut) to save the new password.

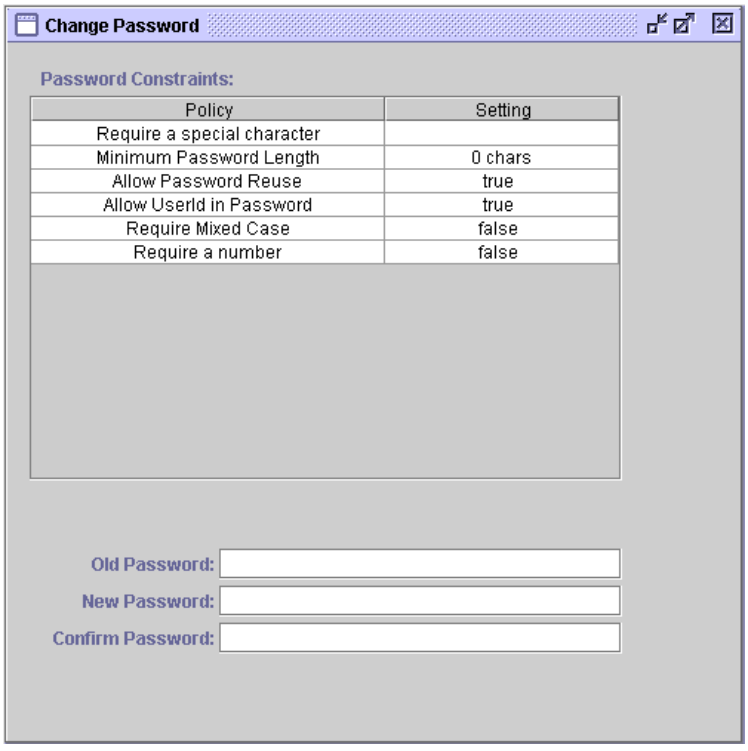

Figure 1-2: Change Password Dialog

Passwords constraints are set according to the following parameters:

Parameter	Description
Require a special character	Requires the use of at least one of the special characters listed. When this field is empty, no special characters are required.
Minimum Password Length	The minimum password length required.
Allow Password Reuse	When set to true, a password can be reused immediately after it has expired. When set to false, users must select a different password each time their password expires. The number of new passwords that must be set before an old password can be reused is defined by the administrator. To view Password History, select *Settings* > *Permissions* > *Application Security Policy* > *Password History*.
Allow UserId in Password	When set to true, allows the password to contain the user ID. When set to false, the use of the user ID in the password is not allowed.
Require Mixed Case	When set to true, the password must include both upper and lower case characters.
Require a number	When set to true, at least one number must be included in the password.

The success of the Login operation also depends on the following Password Policy parameters, set by the system administrator:

Parameter	Description
Password Expiration Age	Determines the period of time that a password is valid. After the password expires, the user must define a new password.
Password History	Defines the number of new passwords that must be used before reusing an old password.

The Password Policy also determines when the user receives a password expiration warning.

To change Password Constraints settings and Password Policy settings, select *Settings* > *Permissions* > *Application Security Policy*. Refer to Section 2.5 for more details.

1.3.7 Disabled Accounts

Users with a disabled account cannot access the system. An account can be disabled by the administrator, or is disabled according to the following Login Policy settings:

- Login Attempts - Number of unsuccessful login attempts before the user is locked out (default: three attempts). The account can be re-enabled by the system administrator, or after the Login Lockout period is over.

- Inactivity Timeout - Interval of time that a terminal can remain inactive before the client is shut down.

- Idle Account Age - Age for disabling an account with no login for the specified period of time. Only the system administrator can re-enable the account.

- Expired Account Age - Age for disabling an active accounts with an expired passwords and no login for the specified period of time. Only the system administrator can re-enable the account.

- Lockout Period - Time user must wait for the account to be enabled again after it was disabled due to the number of unsuccessful login attempts.

To change Login Policy settings, refer to Section 2.5.

To enable an account, Open the User Manager window, select the locked out user and click unlock. Only the system administrator can unlock disabled accounts. See Section 2.2.2.

1.3.8 Application Server

The application server, which typically runs on a dedicated host, enables the system to process incoming alarms and communicate with equipment and network devices. If the client application cannot connect to an application server, a warning message appears and the client is not launched.

1.4 The Home Window

Following a successful Login, the Home window opens. You can also open the Home window by selecting *File* > *Home*, or by clicking the *Home* icon (see Section 1.6.2), or by using the shortcut *Ctrl+H*.

The default *Home* window is the *About* window. You can define any of the windows available through the Navigation pane as the *Home* window, by right-clicking the node in the Navigation pane and selecting *Set As Home Page*.

1.5 The About Window

The *About* window, which is the default *Home* window, displays a list of all products installed and their software version.

To open the *About* window, select *Help* > *About*, or click the *About* icon (see Section 1.6.2).

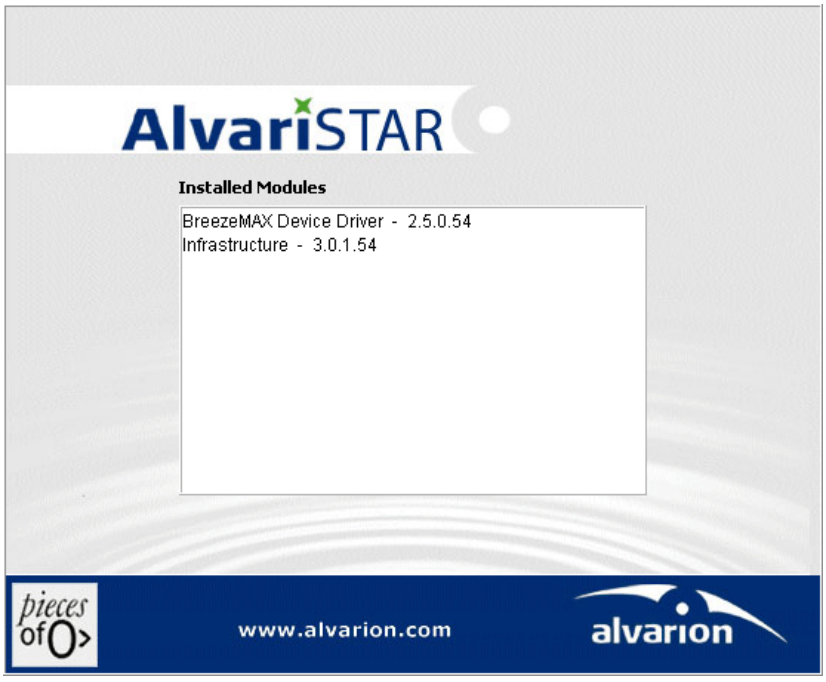

Figure 1-3: About Window

The AlvariSTAR version number and the installed product line device driver version number are in the format a.b.c.d, where a.b increases for major releases, c increases for minor releases and d is an internal control number.

1.6 The Main Window

After logging on to AlvariSTAR, the main window is displayed, providing access to all AlvariSTAR functions.

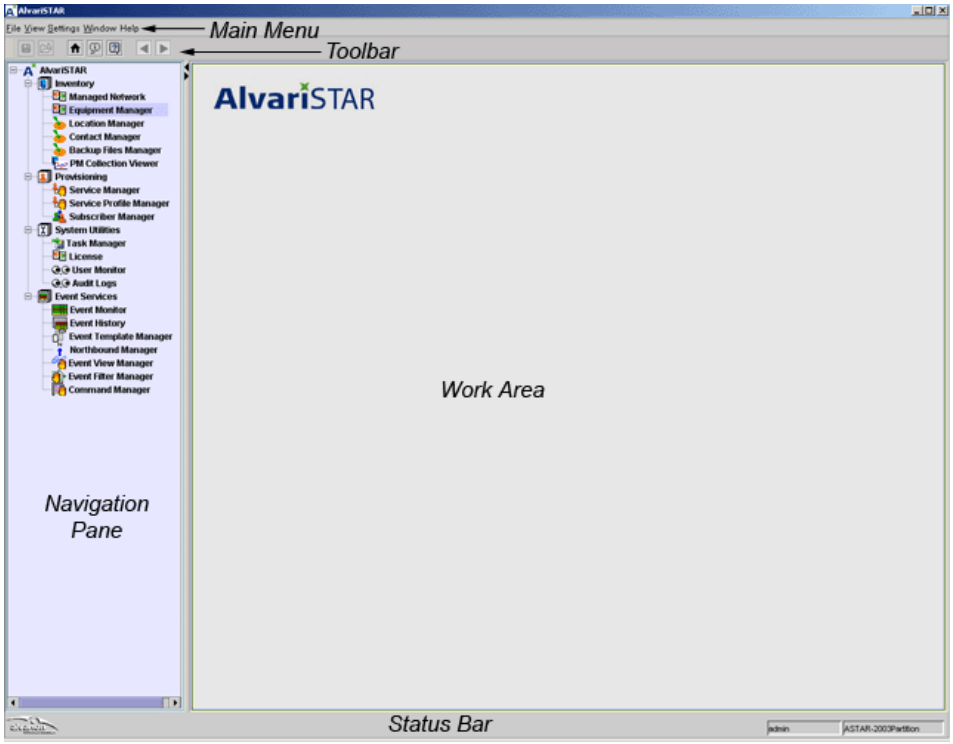

Figure 1-4: AlvariSTAR Main Window

1.6.1 Main Menu

The main menu contains all menus and their options, which provide access to AlvariSTAR functions. It mirrors many of the functions available in the Navigation Pane, and may be displayed with additional options according to the selected item from the Navigation Pane. Commonly encountered menu items are described below:

Menu	Submenu	Description
File	Open	Opens the AlvariSTAR functions menu. It contains all the nodes as displayed in the Navigation Pane. Subnodes and menu items open windows in the work area. It enables access to all the options even when the user chooses to hide the navigation pane. Refer to Section 1.6.3 for more details.
	Home	Returns you to the selected home page. You can also use the *Ctrl+H* shortcut for this option.
	Close	Closes the top window open in the work area. You can also use the *Ctrl+F4* shortcut for this option.
	Close All	Closes all windows open in the work area.
	Save	Saves the changes made in the active window. This function is available only for windows without a Save button. You can also use the *Ctrl+S* shortcut for this option.
	Exit	Closes the client application. You can use *Ctrl+X* as a shortcut for this option. Refer to Section 1.3.5 for more details.
View	Launcher	Enables to choose between MDI View (Multiple Documents Interface) and Browser views. Refer to Section 1.6.4 for more details.
	Navigation	Enables to select whether the Navigation Pane is a tree (default) or a slide menu.
	Show Toolbar	Shows/hides the Toolbar.
	Show Status Bar	Shows/hides the Status Bar.

Menu	Submenu	Description
Settings	Permissions	Enables to view and edit the following permissions. ■ User Manager-Enables to create and manage users, and associate information with each user. ■ User Group Manager-Enables to create and manage user groups. The user groups contain the default access right definitions for all users assigned to that user group. ■ Functional Permissions-Enables to associate system functions (permissions) with individual users or user groups. ■ Application Security Policy-Enables to define policies for user login and passwords. ■ Group Rights Summary-Enables to view a summary of the functional permissions assigned for each user group. For more details refer to Chapter 2. Note: Only Administrators can edit permissions.
	Change Password	Opens the Change Password window, enabling to set a new password for logging in to the application
Window	Enables to select which window appears in the work area if you have more than one window open. It also contains the following options: ■ Next / Prev: Cycles back and forth through the open windows. ■ Cascade / Tile:Enables to align the open windows in tiles or cascade format. Available only when working in MDI View (see Section 1.6.4).	
Help	■ About: Opens the About window. ■ Help: Opens the Help Navigator window and the Help Topic window for the current window. You can also use the *F1* shortcut for this option. ■ Help Topics: Opens the Help Navigator window.	

1.6.2 Toolbar

The toolbar is displayed at all times at the top of the main window and contains quick access icons for some common operations. These icons correspond to the

menu options described in Section 1.6.1. You can hide the toolbar by selecting *Show Toolbar* from the *View* main menu.

Figure 1-5: Toolbar

The icons and the functions they invoke are described below:

Icon	Description
	Save - Saves changes in the open window. *Ctrl+S* is the keyboard shortcut for this function.
	Close - Closes the active/selected window. *Ctrl+F4* is the keyboard shortcut.
	Home - Opens the Home window page. Refer to Section 1.4
	About - Displays the About window. Refer to Section 1.5.
	Help - Opens the Online Help Navigator.
	Prev/Next - Cycles back and forth through the open windows.

1.6.3 Navigation Pane

The application offers two navigational views: Tree View and Slide Menu View.

Figure 1-6: Tree View (left) and Slide Menu View (right)

In either case, click on menu headings to expand that menu node (in tree view, double click on the menu heading or single-click on the **+** sign to its right), then click on the appropriate item in that node to display the associated page.

You can also right-click nodes in this panel to see a context menu with *Set As Home Page, Open,* and *Open in a New Window* options.

The Navigation Pane provides access to all AlvariSTAR functions. The Navigation Pane options are described below:

Node	Description
Inventory	Provides the following sub-menus: ■ Managed Network - Opens the Managed Network Application window, enabling to manage IP address ranges or Subnets and global SNMP Read and Write community pairs. Refer to Section 3.1. ■ Equipment Manager - Opens the Equipment Manager window, enabling to view equipment in the network and access the Equipment Editor. Refer to Section 3.2. ■ Location Manager - Opens the Location Manager window, enabling to define equipment locations and to associate maps and other features with locations. Refer to Section 3.3. ■ Contact Manager - Opens the Contact Manager window, enabling to organize and manage your contacts. Refer to Section 3.4. ■ Backup Files Manager - Opens the Backup Files Manager window, enabling to manage configuration backup files. Refer to Section 3.5. ■ PM Collection Viewer - enables to generate graphs to view collected performance data. Refer to Section 3.6.
Provisioning	Provides several sub-menus that enable to define services and assign them to subscribers. Refer to Chapter 4.
System Utilities	Provides the following sub-menus: ■ Task Manager - Enables to define, manage, schedule, run/abort system-wide operations, such as Network Scan, Database Aging, Configuration Backup, etc. Refer to Section 5.2. ■ License - Enables to view information about valid licenses and summary details on the currently managed device types, included in the license. Refer to Section 5.3. ■ User Monitor - Enables to view information on the currently logged in users and to send messages to a logged in user. Refer to Section 5.4. ■ Audit Logs - Enables to view recorded events and export the logged data to an external Comma Separated Value (CSV) file. Refer to Section 5.5.

Node	Description
Event Services	The Event Services allows you to manage alarms that occur in the network. It displays information about each alarm and lets you acknowledge received alarms. It also provides tools that help you diagnose and correct alarms. The Event Manager is divided into the following sub-menus: ■ Event Monitor - Displays real time updates of new events and alarms entering the system. Refer to Section 6.2. ■ Event History - Queries for alarms and events in the database, according to specified time intervals. Refer to Section 6.3. ■ Event Template Manager - Allows you to create, modify and delete event templates. Refer to Section 6.5. ■ Northbound Manager - Allows you to connect to other management systems and to forward traps related to this system. Refer to Section 6.6. ■ Event View Manager - Allows you to create, edit and delete views. Refer to Section 6.7. ■ Event Filter Manager - Allows you to create, edit and delete filters to the Event Monitor/Event History windows. Refer to Section 6.8. ■ Command Manager - Allows you to create, edit and delete script commands. Refer to Section 6.9.

1.6.3.1 Changing the Navigational View

The application offers two navigational views: Tree View and Slide Menu View.

To change the navigational view:

Select *Navigation* > *Tree View* or *Slide View* from the *View* main menu.

1.6.3.2 Hiding and Displaying the Navigation Pane

By default, both the Navigation Pane and Work Area are displayed. When hovering the mouse over the separation bar between the Navigation Pane and Work Area, the mouse pointer becomes a double-headed arrow (↔). You can change the size of the Navigation Pane by dragging this arrow left/right.

You can hide the Navigation Pane to increase the size of the Work Area or hide the Work area to increase the size of the Navigation Pane by clicking on the arrowheads ( ) located on the separation bar until reaching the required display.

With the Navigation Pane hidden or maximized, if clicking the arrowhead does not restore the display of both panes, manually drag the separation bar to restore the display.

1.6.4 Work Area

The work area displays the application's managers, wizards and editors. You can change the display of the items to be shown as an HTML browser or MDI view, by selecting *View* > *Launcher* from the main menu.

- **Browser View** - Fills the work area with the selected window. Use the Window menu to browse between the open windows.

- **MDI View** - Allows you to see several overlapping windows in the Work Area. Use the Window menu (or the *Ctrl+Tab* shortcut) to toggle between the open windows.

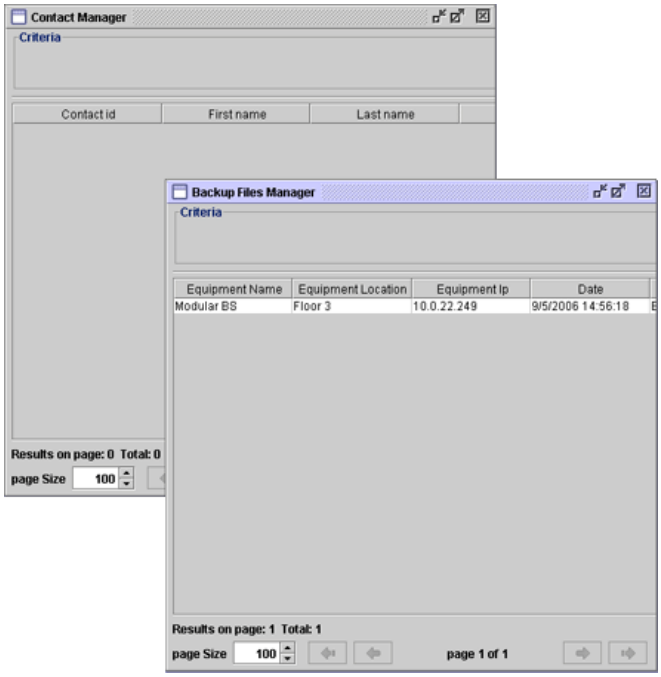

Figure 1-7: MDI View

NOTE

You can cascade and tile MDI windows by selecting *Window* > *Tile* or *Cascade* from the main menu.

In the upper right corner of all MDI windows there are three icons that allow you to minimize, maximize and close the window. Closing the window is equivalent to *Cancel*.

Figure 1-8: Window Control Icons

NOTE

MDI windows may be displayed smaller than the full size, hiding some important information. To view the entire window, use the maximize icon, resize the window to display all the information, or resize table columns (if applicable).

1.6.5 Status Bar

The Status Bar is displayed at the bottom of the main window, and contains the following information:

- Current logged user.
- Partition where the application server is running.

A progress bar is displayed every time a window is refreshed or a new window is selected.

Figure 1-9: Status Bar

To show/hide the Status Bar, select *View* > *Show Status Bar* from the main menu.

1.7 Conventions and Common Operations

The following conventions and common operations appear throughout this manual, unless otherwise specified.

1.7.1 Conventions

The phrase select *Inventory* > *Equipment Manager* from the *File* > *Open* > *AlvariSTAR* menu or the Navigation Pane means you should do one of the following:

- Click on the menu item listed. (*AlvariSTAR* is a sub-item in the *Open* menu item in the *File* menu.)
- Click on the *Inventory* node to expand it in the Navigation Pane, then click on *Equipment Manager*.

1.7.2 Accelerators and Shortcuts

Whenever you see a letter underlined in the title of a menu or button, you can select that menu or button with Alt + [the underlined letter]. Other shortcuts appear in the menus themselves.

1.7.3 Control Buttons

A control button causes an immediate action. To activate a control button, click on it. Certain control buttons only appear in selected windows. Others are common to most windows. Equivalent functions to some control buttons are available from the toolbar and main menu.

Button	Description
Apply	Applies changes made in the window. Clicking the Apply button maintains the window opened for the following transaction or response delivery.
OK	Applies changes made in the window and closes the window.
Cancel	Closes the active window without taking any further action. Any modifications made prior to clicking Cancel are ignored.
Refresh	Refreshes the window and displays the most updated information.
Save	Saves changes made in the dialog box.

Button	Description
Help	Displays the online help window.
Browse	The Browse button appears whenever the command's completion may need additional step. Clicking this button displays another window that lets you select an entry for an adjacent field.
Erase	Clears adjacent fields. It appears next to a field with a Browse button at the other end.
Retrieve	Displays all appropriate matches according to the selected filter. It can also be used to refresh the display.

Some of the control buttons, such as *Edit*, *Open*, *Import* and *Export* may appear grayed out for users without write permission.

1.7.4 Working with Tables

All AlvariSTAR tables and lists allow sorting, resizing and rearranging the column display sequence. In some pages, tables are used for displaying information and configuring and managing multiple entities of the same type.

To modify the configuration of an existing entity:

Double-click on the applicable cell: In a text-cell, edit the content. In some cells a drop-down menu will open, enabling selection of the required option. Click on any other cell to apply the change to the selected cell. At this stage the change is applied only to the display. The change is applied to the device only after clicking on the **Apply** button.

In rows with modified parameter(s) all the details are colored blue.

1.7.4.1 Sorting Tables

Tables can be sorted by clicking on any of the column headings. Click again on a column heading to toggle between ascending and descending sort order.

1.7.4.2 Resizing and Rearranging Columns

To resize a column, position the cursor on the border line between two columns headings. The cursor changes into a double-headed arrow. Drag the cursor to the left or to the right to increase or decrease the size of a column. To rearrange column sequence, click a column header and drag it to the new desired position.

1.7.5 Manipulating the Displayed Information

1.7.5.1 Using Filters

AlvariSTAR supports wildcard characters for specifying entity searches of the various list fields. When applying filters to lists of objects in the application, you can use the asterisk (*) wildcard character as part of the search criteria. The asterisk wildcard character matches any sequence of characters in a string, including an empty sequence.

To apply filters:

1 In the Criteria field, click on the **Browse** button. The filter selection window opens.

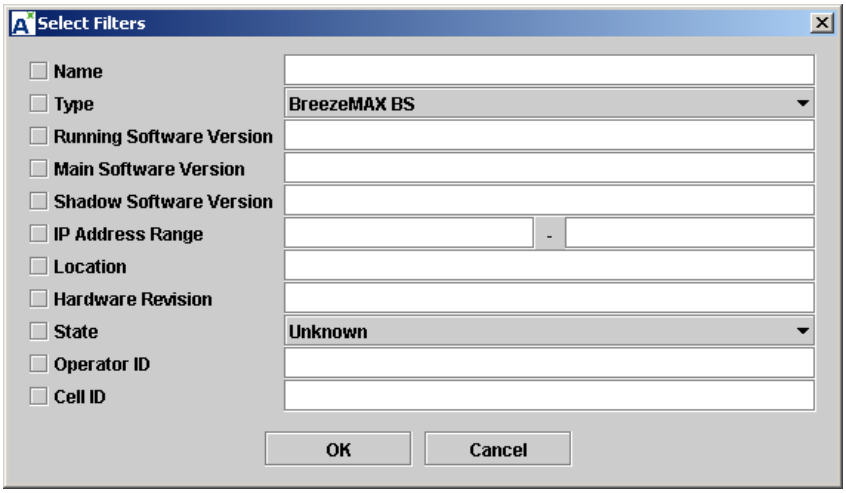

Figure 1-10: Typical Filter Selection Window

2 Select the filter criteria by checking the boxes to the left of each item. If a box is not checked, the field is disabled. To further narrow down the results, select additional filter criteria.

3 For every selected filter criterion, enter a value, or select a value from the drop-down list, as required.

4 Click **OK** to apply the filter criteria.

5 Click on **Retrieve** to complete the filtering and refresh the displayed list.

1.7.5.2 Limiting the Results Set

You can define the maximum number of results to be displayed in a list by entering a number in the *Page Size* box (or *Max Items* in the Event Services windows) or by using the up and down arrows to the right of the number field. The results set will be divided into several pages, according to the set number of Max Rows. Click **Retrieve** to refresh the displayed list.

NOTE

This feature ensures that you do not waste too much time while the application attempts to resolve an unreasonable query. If you cannot narrow the criteria, decrease the maximum result size by selecting a smaller value in the *Max Row* field, to handle the query.

To browse results divided into pages:

When the number of results exceeds the number defined in the *Page Size* box (or *Max Items* box), the results are divided into several pages. Use the following controls to browse the various pages:

Control	Description
	Go to first page.
	Go to previous page.
	Go to next page.
	Go to last page.
	Go to page. Specify the page number in the box to the right.

NOTE

In the Event Services windows, you need to increase the number of *Max Items* to view additional results.

1.8 How to Get Help

Use one of the following options to access the online help:

- Select *Help Topics* from the Help menu or click the Help icon from the toolbar - Opens the Help Navigator window enabling to view help contents, select a specific subject or search for information.

- Click the *Help* button - Opens the Help Navigator window and the Help Topic window according to the open window.

2

Chapter 2 - Permissions

In This Chapter:

- "Overview" on page 30
- "User Manager" on page 31
- "User Group Manager" on page 40
- "Functional Permissions" on page 43
- "Application Security Policy" on page 48
- "Group Rights Summary" on page 54

2.1 Overview

In the Permissions menu you define and manage user permissions and access rights for AlvariSTAR users. The access level you assign to AlvariSTAR users determines which AlvariSTAR management functions that user can access. The Permissions menu provides access to the following windows:

- *User Manager* - Enables to create and manage users, and associate information with each user. Refer to Section 2.2.
- *User Group Manager* - Enables to create and manage user groups. The user groups contain the default access right definitions for all users assigned to that user group. Refer to Section 2.3.
- *Functional Permissions* - Enables to associate system functions (permissions) with individual users or user groups. Refer to Section 2.4.
- *Application Security Policy* - Enables to define policies for user login and passwords. Refer to Section 2.5.
- *Group Rights Summary* - Enables to view a summary of the functional permissions assigned for each user group. Refer to Section 2.6.

2.2 User Manager

This section includes:

- "The User Manager Window" on page 31
- "User Manager Controls" on page 32
- "Adding or Modifying a User" on page 33

2.2.1 The User Manager Window

The AlvariSTAR User Manager, shown below, enables to create and manage users, and associate information to them such as passwords, group membership and contact information. Select *Settings* > *Permissions* > *User Manager* to display the User Manager.

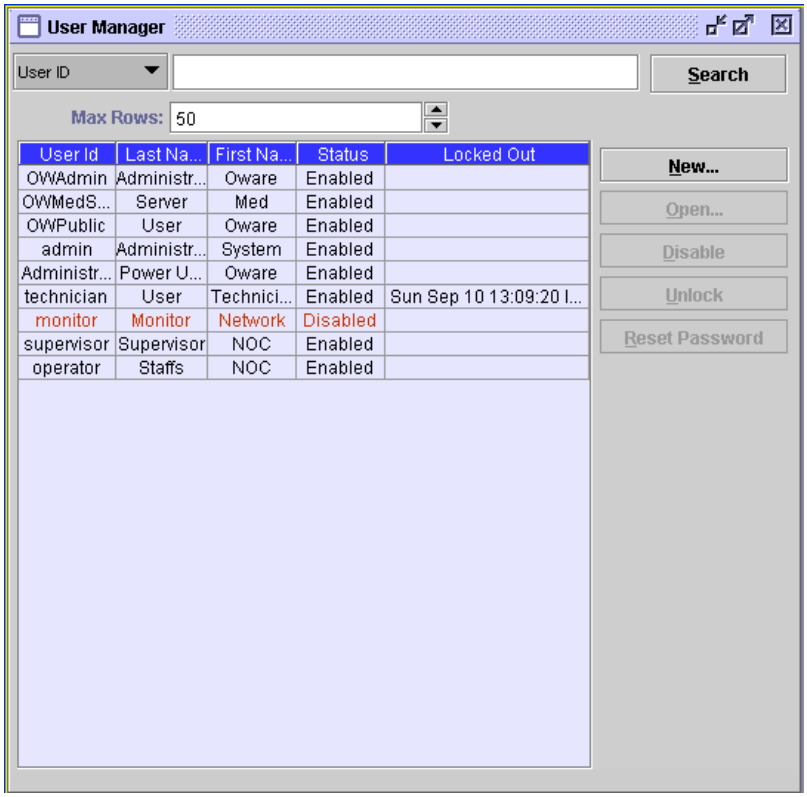

Figure 2-1: User Manager

The User Manager displays the User ID, first and last name, and status (enabled or disabled) for each user, and indicates whether the user is locked out. You can filter the display to show a select subset of users, and can sort so users appear in the order you like.

To filter the display:

Select a filter parameter from the *Filter Menu*, enter the corresponding search text in the text field (case-sensitive), and click **Search**. Use the asterisk (*) as a wildcard to match any number and combination of characters. For example, to display Last Names beginning with C, select *Last Name* and enter *C** in the text field.

If you select *Groups* as the filter criteria, a drop-down menu appears in place of the text field. Select one of the groups from this menu and click **Search**.

To sort the display:

Click on any column header to sort the display based on that column's contents. The initial click sorts the column in ascending order; the next click sorts in descending order. Subsequent clicks toggle the sort between ascending and descending.

2.2.2 User Manager Controls

The User Manager has the following controls:

Parameter	Description
New	Opens a dialog where you can add new users to the system. Refer to Section 2.2.3 for more information.
Open	Opens the user editor populated with the information for the selected user. Refer to Section 2.2.3 for more information.
Disable	Prevents the selected user from logging on to the application by setting the user's Expiration Date to the current date.

Parameter	Description
Unlock	Releases the lock on the selected user. (Locks are indicated by an entry in the *Locked Out* field.) Users can be locked out if they fail to enter the correct password; administrators can configure the number of attempts allowed before users are locked out (see Section 2.5.1). Unless otherwise configured, locked-out users cannot gain entry into the system until an administrator releases their locks.
Reset Password	Resets the password for the selected user. At the next entry, the user will be prompted to change the password.

2.2.3 Adding or Modifying a User

Click **New** to create a new User, or select an existing user and click **Open** to modify that user's properties. A three-tab User Editor appears, open to the General tab.

To create a user:

Click **New** to display the User Editor, enter the appropriate information, and click **Save**. Most of the information associated with a user is optional. However, the following entries are required:

- User ID
- First Name
- Last Name
- Password
- Confirmation of Password

In addition to these entries, you may want to associate the user with a Group. This confers a predetermined set of permissions to the user. See Section 2.2.3.3 for more information.

The three tabs of the User Editor window are:

- "General Tab" on page 34
- "Profile Tab" on page 35

■ “Groups Tab” on page 37

2.2.3.1 General Tab

The General tab lets you enter and edit identifying and contact information for the selected (or newly created) user.

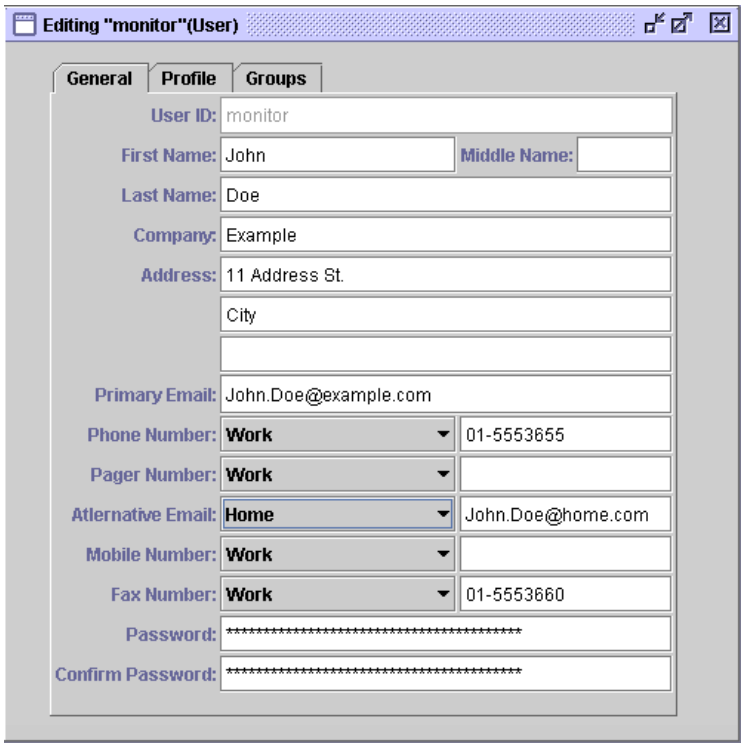

Figure 2-2: User Manager: General Tab

The following are the fields on this tab (described when not self-evident):

Parameter	Description
User ID	(Required) Enter an ID for this user. If you are modifying an existing user, this field is read-only. The User ID must be unique; if it matches an existing User ID, the application generates an error. The User ID you enter here is the User ID displayed in the User Manager window (see Section 2.2) and in all relevant AlvariSTAR reports.
First Name	Type in the User’s first name.
Middle Name	Type in the User’s middle name. The middle name may be used as a secondary identifier with which to identify the user.
Last Name	Type in the User’s Last name.

Parameter	Description
Company	Type in the User's company name.
Address	Type in the User's postal address.
Primary Email	Type in the User's main email address.
Phone Number	Select a phone number type from the drop-down list, then type in a phone number for the selected user.
Pager Number	Select a pager number type from the drop-down list, then type in a pager number for the selected user.
Alternative Email	Select an email type from the drop-down list, then type in an alternate email for the selected user.
Mobile Number	Select a mobile number type from the drop-down list, then type in a mobile number for the selected user.
Fax Number	Select a fax number type from the drop-down list, then type in a fax number for the user.
Password	(Required) Enter the password for this user. For security purposes, the characters appear as a series of asterisks. The default security does not require the password to contain mixed-case letters, numbers, or special characters. Once a user has been created, this field becomes read-only.
Confirm Password	(Required) Re-enter the password for this user. If this entry does not match the Password entry, an error dialog appears and both password fields empty.

2.2.3.2 Profile Tab

The Profile tab provides access to password and login parameters like expiration policy and expiration date, and lets Administrators reset the expiration dates of locked-out users.

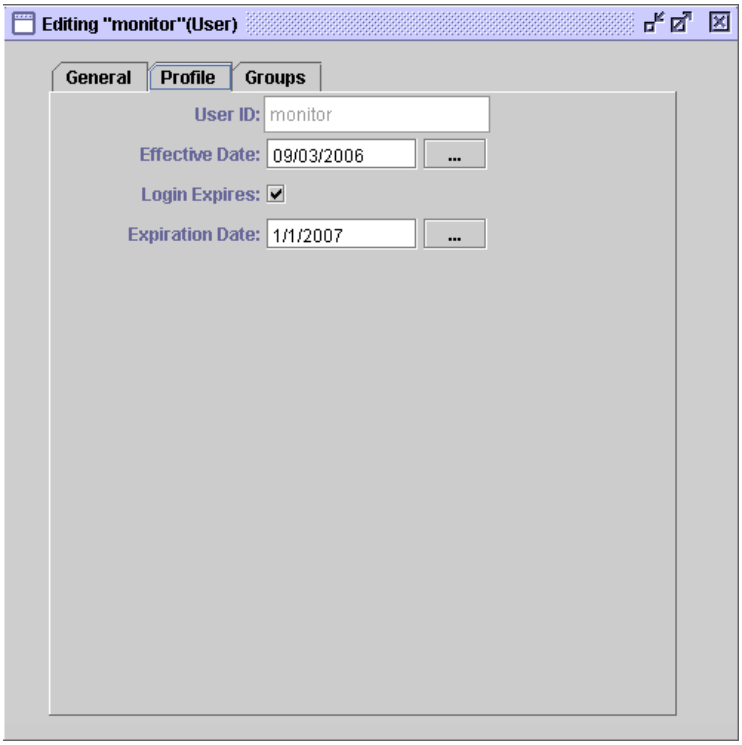

Figure 2-3: Profile Tab

The Profile tab includes the following fields:

Parameter	Description
User ID	The (read-only) ID for the selected user.
Effective Date	(Required) The date when this account becomes effective. This field lets you create accounts in advance. The accounts remain dormant until the Effective Date arrives. Specify an Effective Date by entering the date directly in the text field, in the proper format (by default: month/day/year). You can also click the **Browse** button (...) and select a date from the calendar graphic display.
Login Expires	Indicates whether the login for this user expires. If you select this option, the application activates the Expiration Date field.

Parameter	Description
Expiration Date	Specifies the date on which the login expires. This field is not active unless you select the Login Expires option. Specify an expiration date by entering the date directly in the text field, in the proper format (by default: month/day/year). You can also click the **Browse** button (...) and select a date from the calendar graphic display. If a user is disabled, typically by login failure, the Expiration Date becomes the current date. The user cannot log in again until you reset the Expiration Date to some future date or clear the *Login Expires* option.

2.2.3.3 Groups Tab

The Groups tab lets you determine which user groups, if any, to associate with a user (see Section 2.3 for information about how to create the groups that appear here). As you grant permissions to defined groups, you can grant or deny users access to certain functions based on their group associations.

The ID for the selected user appears at the top of the tab. Available groups appear in the left tab, and groups currently assigned to the selected user appear in the right tab.

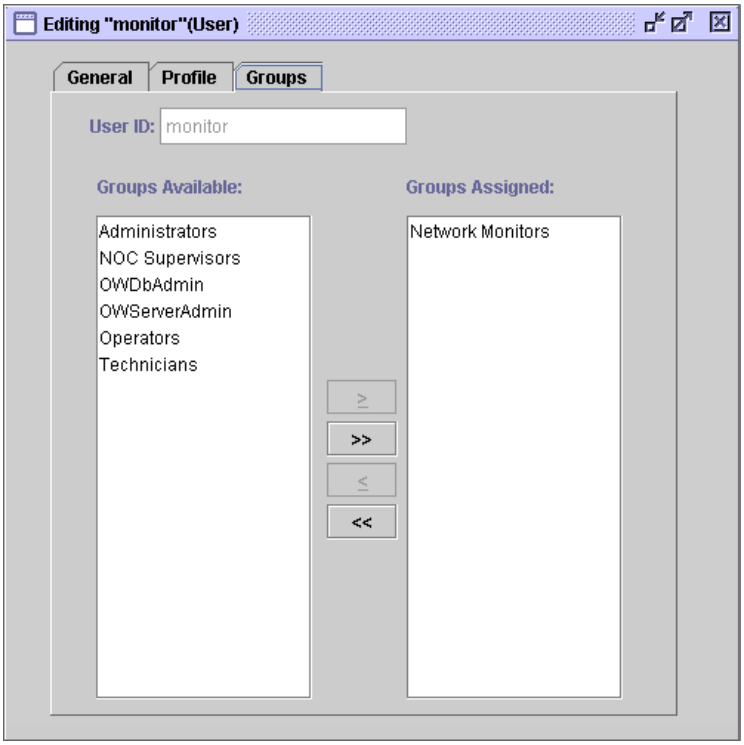

Figure 2-4: Groups Tab

Use the controls in this tab to assign groups to or remove assignments from the current user.

To Add Group Assignments:

Select one or more groups from the left pane (*Groups Available*) and click the right-arrow (**>**) button to move those groups into the right pane (*Groups Assigned*). Ctrl+click to select multiple non-contiguous items, or click on one item and Shift-click on another to select a range of consecutive items. Click the double-right-arrow (>>) button to move all of the groups from the left to the right pane. Select **Save** from the File menu (or use the shortcut *Ctrl+S*) to store your changes.

To Remove Group Assignments:

Select one or more groups from the right (Groups Assigned) pane and click the left-arrow (**<**) button to move those groups into the left pane. Ctrl+click to select multiple non-contiguous items, or click on one item and Shift-click on another to

select a range of consecutive items. Click the double-left-arrow (<<) button to move all of the groups from the right to the left pane. Select Save from the File menu (or use the shortcut *Ctrl+S*) to store your changes.

2.3 User Group Manager

The User Group Manager lets you create user groups (see “User Manager” on page 31 for instructions about creating users). Open this manager from *Settings* > *Permissions* > *User Group Manager*. Initially, a Group is nothing more than a name and a description.

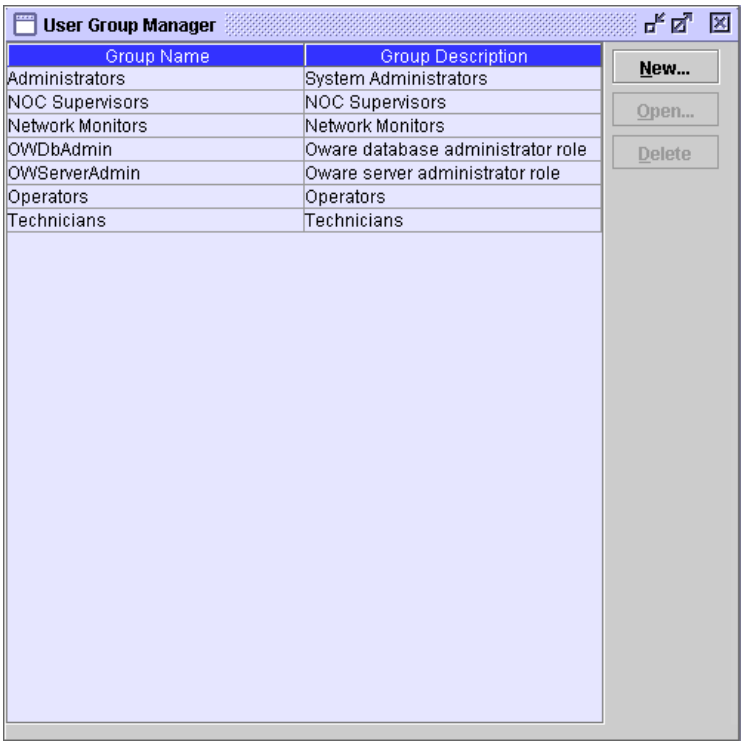

Figure 2-5: User Group Manager

Once created, however, you can associate individual users with groups (See Section 2.2.3.3), and grant permissions to users based on their association with a group (See Section 2.4).

For more information on using the User Group Manager, refer to:

- “Adding or Modifying a Group” on page 41
- “Deleting a Group” on page 42
- “Default User Groups and Users” on page 42

2.3.1 Adding or Modifying a Group

Adding groups and modifying groups are similar operations using the same interface.

To add a new group:

Click **New**.

To modify an existing group:

Select the group in the Group Manager, and click **Open**.

In both cases, an editor window (shown below) appears. If you are editing an existing group, the window contains the information for that group. If you are creating a new group, the window is blank.

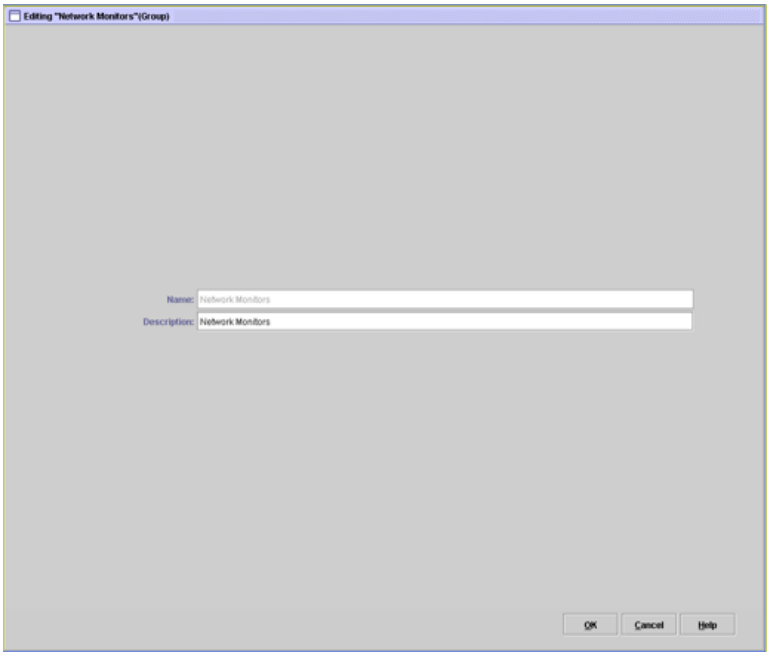

Figure 2-6: Group Editor

Enter or modify the appropriate information in the Group Editor's fields and click **OK** to save the entry. The following are the fields in this window:

Parameter	Description
Name	The name of the group (read-only if editing). This entry is obligatory, and must be unique.
Description	A description of the group. This entry is optional.

2.3.2 Deleting a Group

Select the group in the Group Manager and click **Delete**.

2.3.3 Default User Groups and Users

By default, several user groups with one user defined in each group are provided when you install your application. The following are the defaults:

Parameter	Description
Administrators	admin
NOC Supervisors	supervisor
Network Monitors	monitor
Operators	operator
Technicians	technician

NOTE

Additional groups include: OWadmin, OWMedServer, and OWPublic.

2.4 Functional Permissions

Functional permissions lets you associate system functions (permissions) with individual users or with user groups.

Typically, the functional permissions defined for the various user types provide the following capabilities:

Parameter	Description
Administrator	Access to all Network Management functionality.
NOC Supervisor	Access to all functionality except Access Rights management.
Operators	Access to Fault and Configuration management for single and multiple devices.
Technicians	Access to Fault and Configuration management.
Network Monitors	Access to Fault and Configuration management for view only (Read Only).

This section includes:

- "The Functional Permissions Page" on page 43
- "Function Associations" on page 45
- "Functional Permissions Editor" on page 45

2.4.1 The Functional Permissions Page

Select *Settings* > *Permissions* > *Functional Permissions* to display the Functional Permissions page, shown below.

Functional permissions are global and additive with other permissions. If you have a group permission and a functional permission set, the result is a union, not an intersection of the two.

Grant permissions by selecting a predefined function and then create a list of groups and/or individual users authorized to perform that function. You can further refine permissions by defining a set of actions (read, write, execute, and so on) that each group or user can perform when exercising the function.

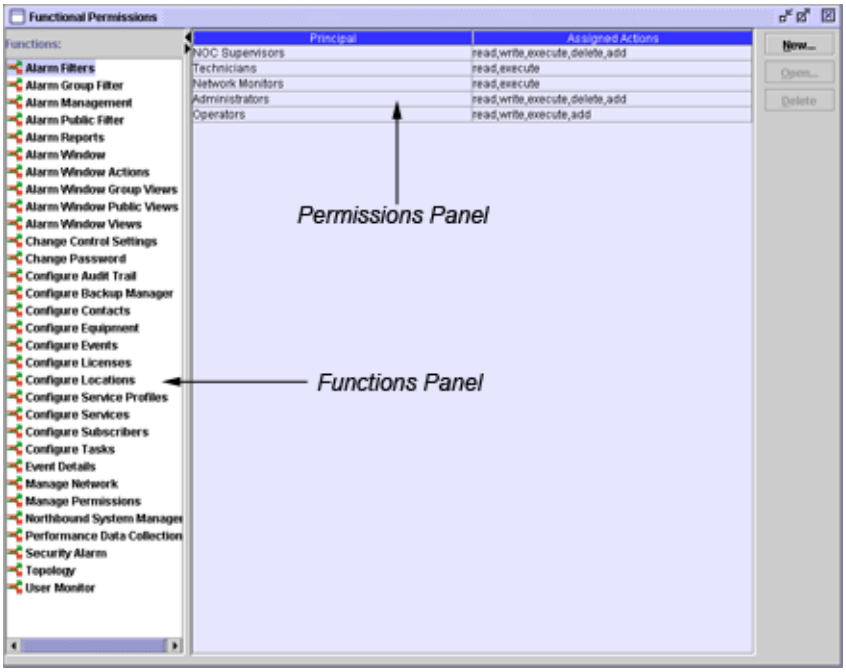

Figure 2-7: Functional Permissions Page

The following panels are available in the Functional Permissions page:

- **Functions Panel** — The Functions panel displays the available functions. Select a function by clicking it; the groups and users who have been granted permission to perform this function appear in the Permissions Panel, along with the permitted actions (read, write, execute and delete, for example.)
- **Permissions Panel** — The Permissions panel displays the Principal (the groups) allowed to perform the selected function in the Functions page, and the Assigned Actions for each group or individual associated with that function.

Parameter	Description
New	Enables to associate a new Principal with the selected function and assign actions to that Principal. Clicking *New* opens the Functional Permissions editor with the *Principal* (Group) drop-down menu active.
Open	Enables to open an existing permission.
Delete	Enables to delete an existing permission.

Possible functional permissions authorize the following:

Parameter	Description
read	Retrieve data from the database.
write	Update data in the database.
execute	Execute some application function.
delete	Delete data from the database.
add	Create new data.

2.4.2 Function Associations

You can do the following with the association of Groups or Principals with functions:

- **Associate a New Principal or Group with a Function**—Select a function in the Function page of the Functional Permissions Manager and click **New**.
- **Modify Actions Permitted a Principal or Group for a Function**—Select a function in the Function page of the Functional Permissions Manager. Select the *Principal* or *Group* for which you want to modify the assigned actions and click **Open**.
- **Remove Associations Between Principal or Group and a Function**—Select a function in the Function page of the Functional Permissions Manager, select the *Principal* or *Group* whose association you want to remove and click **Delete**.

2.4.3 Functional Permissions Editor

You can change the functional permissions through the Functional Permissions editor, as shown in Figure 2-8 below.

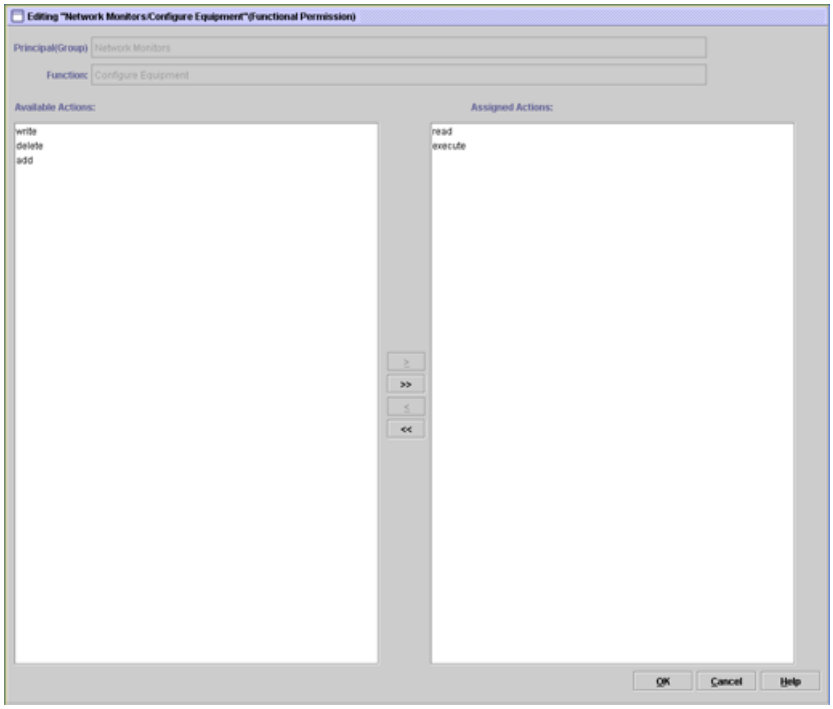

Figure 2-8: Functional Permissions Editor

The *Functional Permissions Editor* includes the following fields:

Parameter	Description
Principal (Group/User)	Drop-down menu (when adding a new Principal) from which you can select a User Group or individual. The *Show Groups/Show Users* button determines the state of this menu (groups or individuals), and the menu displays its state in the parenthetical expression. If the menu is in *Users* mode, the title reads *Principal(User)*. If it is in *Groups* mode, the title reads *Principal(Groups)*. During Edit operations, the *Principal* field is a read-only area (and not a menu) that displays the Principal (either a Group or a User) whose permissions you are editing.
Show Groups/Show Users	Mode selector for the *Principal* menu. Click this button to change the mode of the Principal menu from Groups to Users, or vice versa. If the Principal menu is in *Groups* mode, this button reads *Show Users*. If the Principal menu is in *Users* mode, this button reads *Shows Groups*.
Function	This read-only field displays the function whose associations or permissions you are editing.

Parameter	Description
Available Actions	Displays a list of actions available, but not assigned, for the selected function. To assign actions from this list to the current group or user, select one or more actions and click the underlined right (**>**) arrow. Assign all the available actions by clicking the double right arrow (**>>**).
Assigned Actions	Displays a list of actions assigned, for this function, to the current group or user. To remove assigned actions, select one or more from the list and click the underlined left (**<**) arrow. Remove all assigned actions by clicking the double left arrow (**<<**).

Click **OK** to implement any changes you have made, or click **Cancel** to close the dialog and discard your changes.

2.5 Application Security Policy

The Application Security interface lets you specify security policies governing user login and passwords. Open the Application Security Policy page by selecting *Settings* > *Permissions* > *Application Security Policy*.

The following are types of application security policies described in this section:

- "Login Policy" on page 48
- "Password Policy" on page 50
- "Password Constraint" on page 52

2.5.1 Login Policy

The Login Policy section of the Application Security Policy page sets policies for user logins. These policies govern the message that appears in the login screen and the various security measures applied to user's attempts to log in.

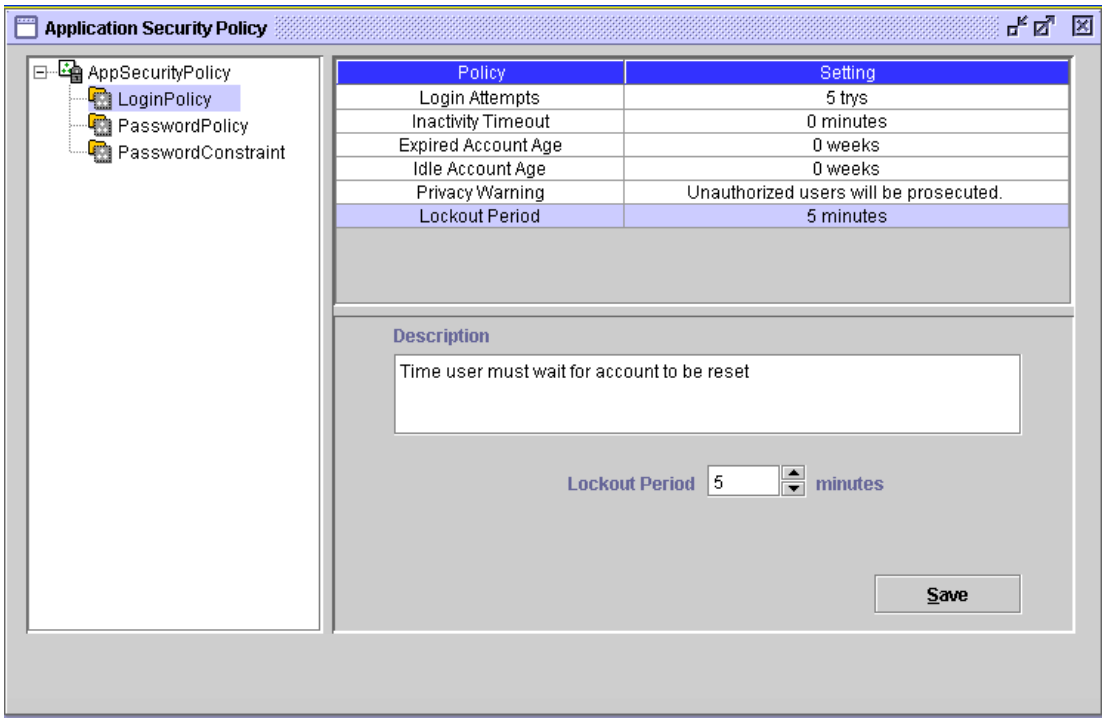

Figure 2-9: Login Policy Page

The individual policies available from the Login Policy Page are listed below.

Each Login Policy appears in the list along with its current setting. Edit a policy by clicking it; an editor appropriate to that setting appears in the lower portion of the page.

Login Policy includes the following properties:

- Idle Account Age
- Expired Account Age
- Lockout Period
- Privacy Warning
- Inactivity Timeout
- Login Attempts

2.5.1.1 Idle Account Age

The Idle Account Age determines how long an account can remain inactive (have no logins) before it is disabled.

2.5.1.2 Expired Account Age

The Expired Account Age setting determines how many weeks an account can remain active if it has an expired password and no logins. Once this threshold is reached, the account is disabled and can only be reactivated by an administrator.

2.5.1.3 Lockout Period

The Lockout Period determines how long a user must wait, after a failed login attempt, before a new attempt is allowed.

2.5.1.4 Privacy Warning

The Privacy Warning appears every time a user logs in. Enter your text in the Privacy Warning field and click **Save** to implement the change.

2.5.1.5 Inactivity Timeout

The Inactivity Timeout setting determines how long a terminal can remain inactive before the client is shut down. A setting of 0 effectively disables this setting, allowing users to remain inactive indefinitely.

2.5.1.6 Login Attempts

The Login Attempts setting specifies how many consecutive unsuccessful login attempts are allowed before a user is locked out.

2.5.2 Password Policy

The settings associated with Password Policy determine whether (and how long) users can keep passwords, how many unique passwords a user must have before the oldest can be re-used, and how much warning they get before their password expires.

Display the password policies by clicking the Password Policy icon in the navigation page. The individual policies appear in the right-hand page.

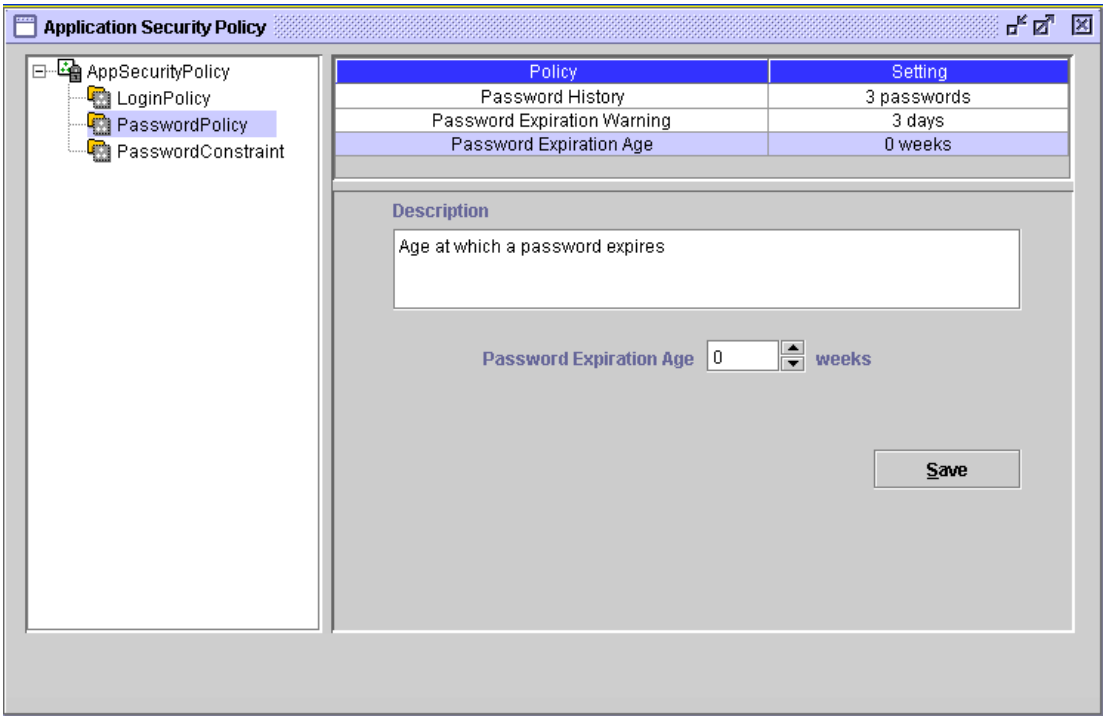

Figure 2-10: Application Security Policy Page — Password Policies

Edit a policy by clicking it; an editor appropriate to that policy appears in the lower portion of the page.

Password Policy includes the following properties:

- Password Expiration Age
- Password History

- Password Expiration Warning

2.5.2.1 Password Expiration Age

The Password Expiration Age setting determines how long a user can keep a password before a new one must be selected. Enter a value directly in the Password Expiration Age field, or use the up and down arrows to change the displayed value.

2.5.2.2 Password History

Enter the *Password History* setting in conjunction with the *Allow Password Reuse* setting (see Section 2.5.3.6). If password reuse is not allowed, the system tracks passwords in a FIFO (First In, First Out) queue, up to the number specified by this setting.

You can reuse an old password after the specified number of other passwords have been used. For example: If you do not enable *Allow Password Reuse* and Password History is set to three, a user's sequence of passwords might look like this:

House*Magnet

Fig@Bumper

Rose-Window

Standard+Disclaimer

House*Magnet

You can reuse `House*Magnet`, since three other passwords have been used since `House*Magnet`.

NOTE

A setting of zero, as shown in the example, effectively enables immediate password reuse even if you do not set Allow Password Reuse.

2.5.2.3 Password Expiration Warning

The Password Expiration Warning page enables to set the number of days in which the user will be notified before his password expires. At login, the user will be prompted to change the password. Enter a value directly in the *Password Expiration Warning* field, or use the up and down arrows to change the displayed value.

2.5.3 Password Constraint

Password Constraint policies specify how to construct passwords. Display them by clicking the Password Constraint icon in the navigation page. The display shows each policy and its current setting. Edit a policy by selecting it; the edit dialog appears in the lower portion of the page.

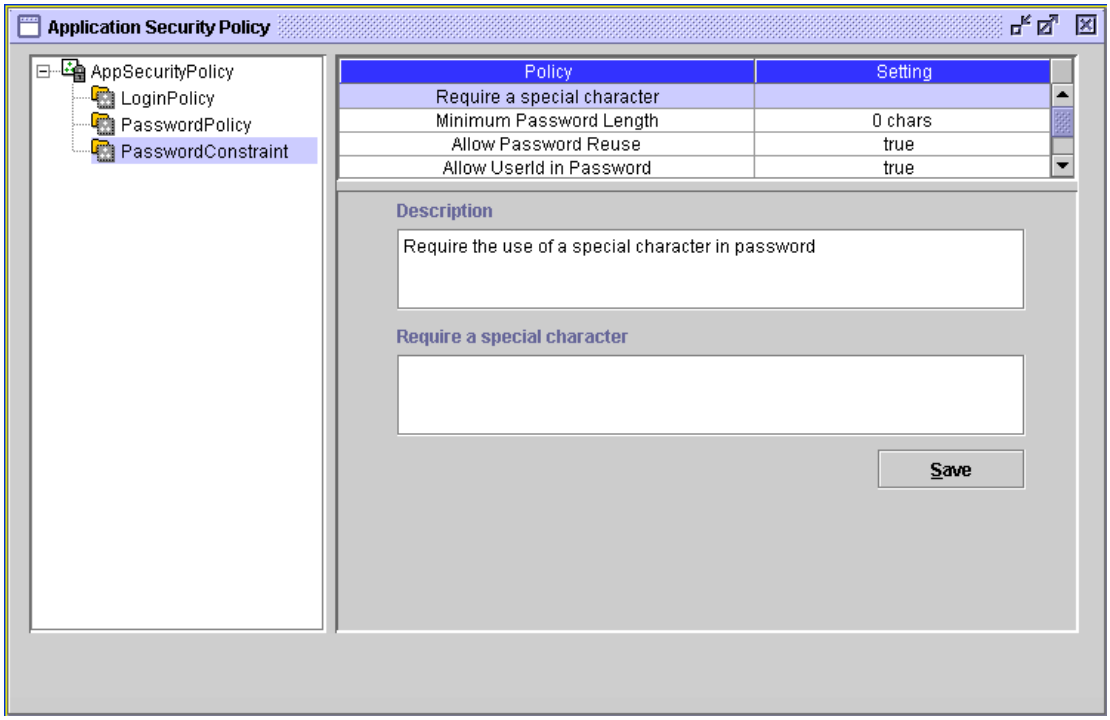

Figure 2-11: Password Constraint

Password Constraint includes the following properties:

- Require Mixed Case
- Minimum Password Length
- Require a special character
- Allow UserId in Password
- Require a number
- Allow Password Reuse

2.5.3.1 Require Mixed Case

This requires a user's password to include both upper and lowercase characters — `HouseMagnet`, for example.

2.5.3.2 Minimum Password Length

This setting specifies the minimum length of a password. Enter a value directly in the *Minimum Password Length* field, or click the up or down arrows to change the displayed value.

NOTE

Blank passwords are not accepted even if the minimum length is set to 0 (zero).

2.5.3.3 Require a special character

This requires a special character to be part of a user's password — house*magnet, for example. Activate this option by entering the special characters considered acceptable in the *Require a special character* field. In the example above, an asterisk (*) is among the acceptable special characters.

2.5.3.4 Allow UserId in Password

This lets users include their User ID in their passwords. For example, user MyUser could create *house*MyUser*magnet* as a password.

2.5.3.5 Require a number

This specifies whether users must include a number in their passwords — *house2magnet*, for example.

2.5.3.6 Allow Password Reuse

This determines whether users can reuse their password immediately after it has expired. If this option is not selected, users must select a different password each time their password expires. The number of new passwords that must be used before an old password is reused is then determined by the Password History field, see Section 2.5.2.2.

2.6 Group Rights Summary

The Group Rights Summary page provides a read-only summary of user groups, as defined in Section 2.3, and each group's assigned functions and actions, as defined in Section 2.4.3.

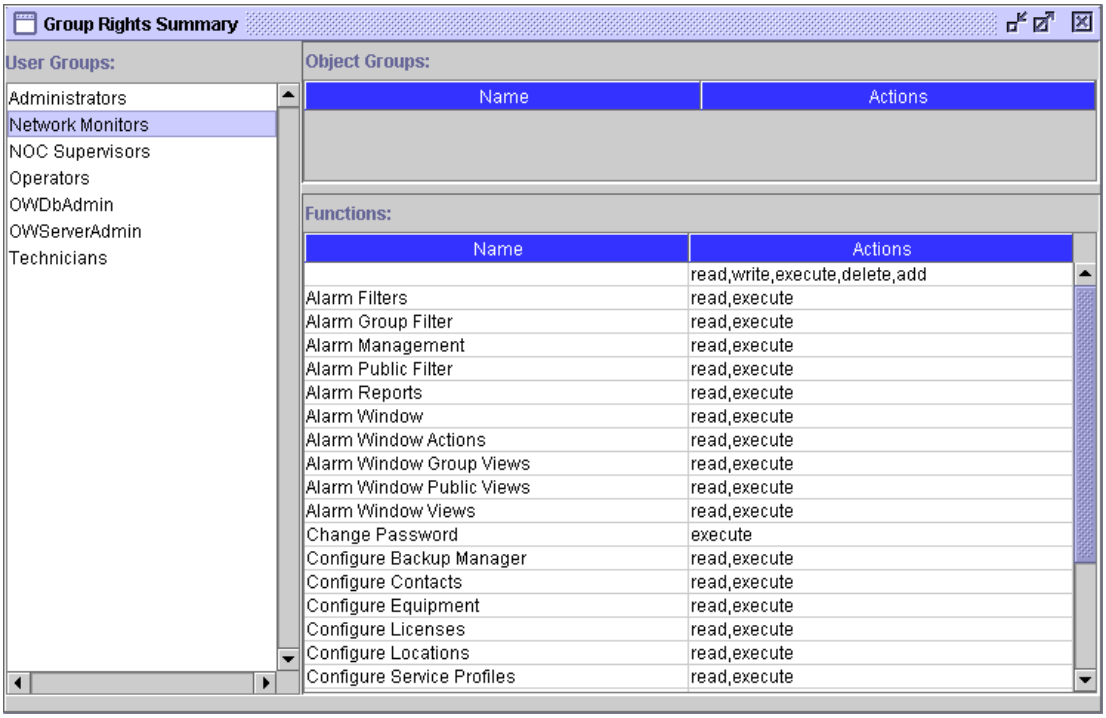

Figure 2-12: Group Rights Summary Page

To display the information for a user group, select that group in the left (User Groups) page.

3

Chapter 3 - Inventory

In This Chapter:

- "Managed Network" on page 56
- "Equipment Manager" on page 61
- "Location Manager" - Section 3.3
- "Contact Manager" on page 74
- "Backup Files Manager" on page 77
- "PM Collection Viewer" on page 81

3.1 Managed Network

The Managed Network Application enables to define the IP ranges in which devices are expected to be discovered, and global SNMP Read and Write community pairs. This defines the scope of your network and only devices within this scope will be discovered. Up to 65535 IPs are supported.

To open the Managed Network Application:

Select *Inventory* > *Managed Network* from the *File* > *Open* > *AlvariSTAR* menu or the Navigation Pane. The Managed Network Application includes two tabs:

- "Network IP Address Ranges Tab" - Section 3.1.1
- "Network Communities Tab" - Section 3.1.2

3.1.1 Network IP Address Ranges Tab

The *Network IP Address Ranges* tab displays the currently defined IP address ranges (up to 65535 IPs) and other applicable information and enables to add, edit, or remove a range.

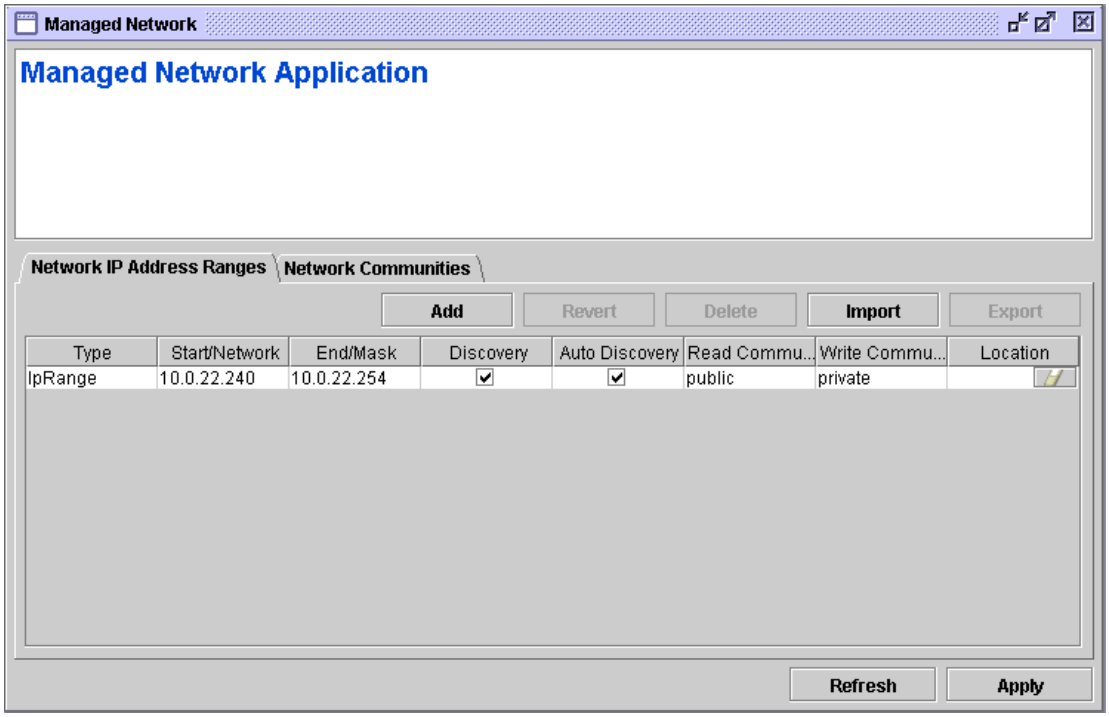

Figure 3-1: Network IP Address Ranges Tab

You can edit the Network IP Address Ranges table by clicking inside the cells and entering the required information. The following information is displayed for each range:

Parameter	Description
Type	The type of range definition: IP Range or Subnet. Select from the drop-down menu whether to define the range using IP Range (the first and last address in the range) or Subnet (Network and Mask).
Start/Network	The first IP address in an IP Range or the Subnet address in a Subnet range type.
End/Mask	The last IP address in an IP Range or the Subnet Mask in a Subnet range type.

NOTE

To minimize unnecessary traffic load in the network, avoid defining IP address ranges that include too many “gaps”, e.g., non existing addresses.

Parameter	Description
Discovery	Check to enable periodical discovery, according to parameters defined in the Task Manager. When unchecked, discovery is disabled.
Auto Discovery	Indicates whether Auto Discovery for the range is enabled or disabled. When enabled, Discovery will be initiated whenever a trap is received from a device in the range.
Read Community	The unique SNMP Read community to be used by discovery when accessing devices in the range. If unique communities are not defined, the defined global Read communities will be used one after the other.
Write Community	The unique SNMP Write community to be used when accessing discovered devices in the range. If unique communities are not defined, the global Write community paired with the global Read community that was used to discover devices in the range will be used when accessing these devices.
Location	The location defined for devices in the range. If a location is not defined, the range will be used as the default location.

NOTE

Whenever possible, use unique SNMP community pairs for defined ranges rather than global community pairs.The key for deciding which Write community to use is the IP range. Unique community definitions enable to use the same Read community with several different Write communities in different ranges, as well as to use the same Write community with several different Read communities in different ranges. When using global community pairs, the Read community is the key for deciding which Write community to use, meaning that the Read community should not be used in more than one pair.

The Discovery process is based on the defined Read community. All future device management actions will use the defined Write community. If a wrong Write community was defined, the device will be discovered and displayed, but its status will be “Unknown” and it will not be possible to manage it. The same is true for cases where the Write community in the device was changed (not through AlvariSTAR) after being discovered. In this case, the range must be updated with the correct Write community, the device(s) must be deleted from the database, and the Discovery process for the range should be re-initiated.

The Network IP Address Ranges tab contains the following buttons:

Parameter	Description
Add	Click to add an empty row to the Network IP Address Ranges table. Proceed by entering the required information in each table cell. Click **Apply** to save your changes. Up to 65535 IPs are supported.
Revert	Reverts the table to the last save, discarding any unsaved changes.
Delete	Click to delete the selected Network IP Address Range entry.
Import	Click to import an existing file (.nar) of IP address ranges settings. Browse to the location of the file and click **Open**.
Export	Click to export the current IP Address Ranges table to an external file (.nar). Browse to the location where the file is to be saved and click **Save**.

3.1.2 Network Communities Tab

The Network Communities tab displays the currently defined global SNMP Read and Write community pairs and enables to add, edit, and delete a community pair. Global community pairs are used when a unique pair is not defined for an IP address range.

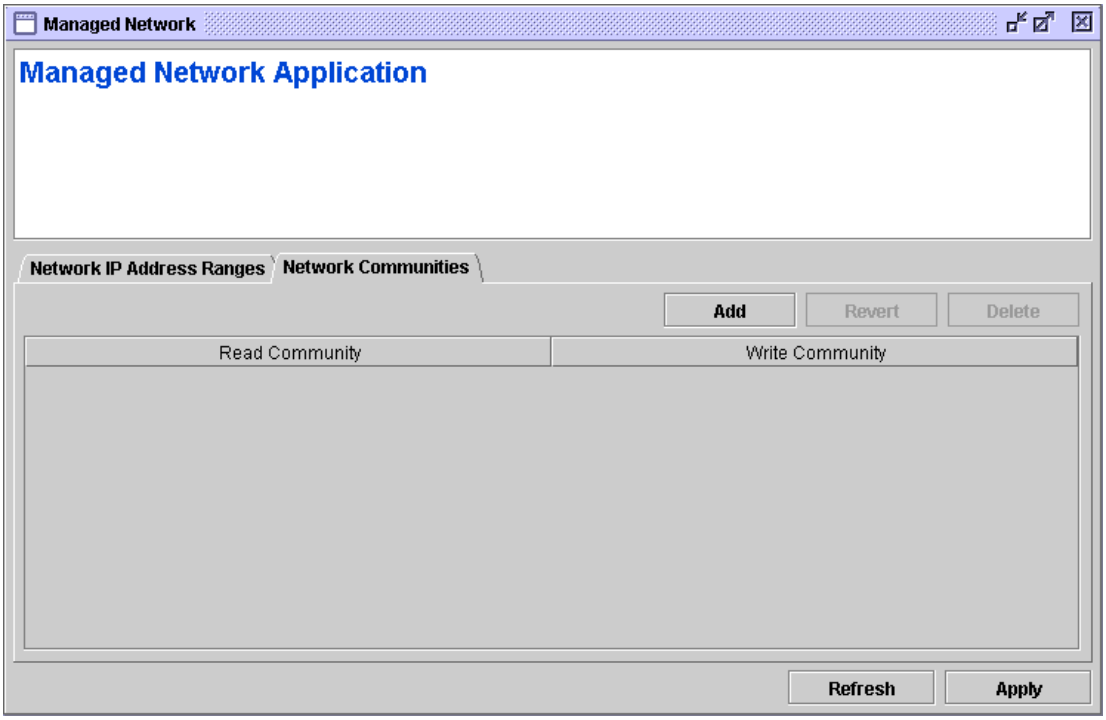

Figure 3-2: Network Communities Tab

You can edit the Network Communities table by clicking inside the cells and entering the required information. The following fields are displayed for each pair:

Parameter	Description
Read Community	A global SNMP Read Community to be used by discovery when accessing devices in a range for which no unique community pair is defined. The global Read Communities will be used one after the other until getting a response from the device or until all of them have been tried.
Write Community	The SNMP Write community to be used when accessing devices that were discovered using the paired Read Community.

The Network Communities tab contains the following buttons:

Parameter	Description
Add	Click to add an empty row to the Network Communities table. Proceed by entering the required information in each table cell. Click **Apply** to save your changes.
Revert	Reverts the table to the last save, discarding any unsaved changes.
Delete	Click to delete the selected Network Network Community pair.

NOTE

When using global community pairs, the Read community is the key for deciding which Write community to use. Each Read community should not be used more than once.

3.2 Equipment Manager

The Equipment Manager provides functionality and access to windows that let you manage equipment in your network. From the Equipment Manager you can:

- View devices that exist in the database according to various selection criteria
- View general information on the displayed devices
- Add, Edit and Delete devices from the database
- Open the Configuration window to configure a selected device
- Open the Multiple Configuration window to configure several selected devices
- Apply licenses to selected equipment
- Open a Telnet session for a selected device
- Backup the configuration of selected devices
- Export the general information of selected devices to a Commas Separated Value (CSV) file.
- Open a map display associated with the device, if applicable.

To open the Equipment Manager:

Select *Inventory* > *Equipment Manager* from the *File* > *Open* > *AlvariSTAR* menu or the Navigation Pane. The Equipment Manager window is displayed.

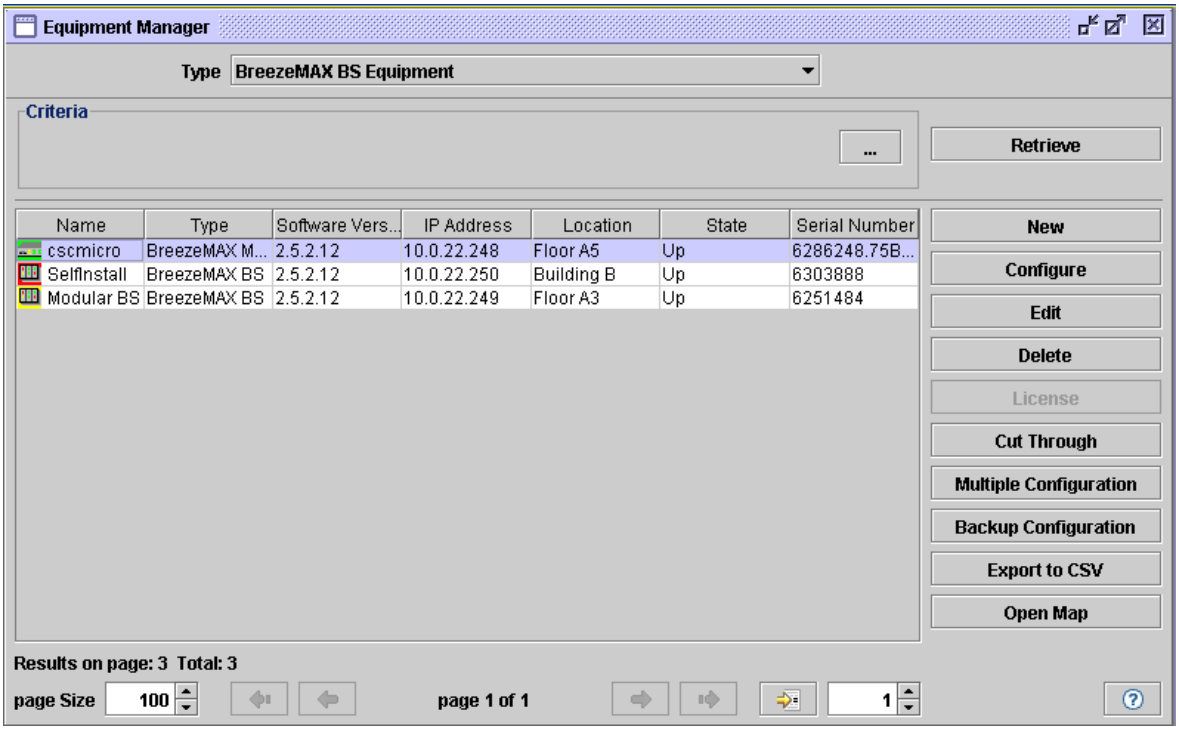

Figure 3-3: Equipment Manager

The Equipment Manager displays a list of all the devices in the database. You can use the Criteria filters to narrow down the search parameters.

The Equipment Manager window displays general information for each of the devices found according to the selected *Criteria* scheme. The background color of the device's icon is in accordance with the device's alarm status (the highest severity open alarms). For more information, refer to "Alarm Severities" - Section 6.4.2.

For each device, the following information is displayed:

Parameter	Description
Name	The name of the device.
Type	The type of device: BreezeMAX BS, BreezeMAX MBS, BreezeMAX SU.
Running SW Ver	The running software version of the device.
IP Address	The IP address of the Device (for BreezeMAX SU - the IP address of the Base Station).
Location	The location associated with the equipment.

Parameter	Description
State	The operational state of the equipment: Up/Down/Unreacheable/ Unlicensed/Unknown
Serial Number	The serial number of the equipment.
MAC Address	The SU's MAC address. Displayed for SUs only.
CPE Type	The SU Type: CPE, CPE-Si, CPE-PRO. Displayed for SUs only.
NG Present	Indicates whether or not a Networking Gateway (NG) is present. True/False. Displayed for SUs only.
VG Present	Indicates whether or not a Voice Gateway (VG) is present. True/False. Displayed for SUs only.

The following are the controls on the Equipment Manager window:

Parameter	Description
New	Adds a new Base Station to the list of Equipment. Click to select the type of equipment to be added: BreezeMAX BS or BreezeMAX MBS. Click **OK**. The Equipment Editor opens, allowing to enter general information on the Base Station.
Configure	Opens the Configuration window, allowing to configure the selected device. Not available if more than one device are selected or if the State is other than Up. For more details, see the *Device Manager User Manual*.
Edit	Opens the Equipment Editor for the selected equipment object, allowing to edit general information. You can edit only the location and contact of SUs and of multiple selected devices. For more details, see Section 3.2.2.
Delete	Deletes the selected equipment object(s) from the database. Select the device(s) to remove and click **Delete**. The application prompts you for confirmation. You can always rediscover deleted equipment. SUs with operational state Up, cannot be deleted.
License	Activated only when unlicensed equipment is selected. Unlicensed equipment cannot be managed by AlvariSTAR. Enables to apply a license to the equipment, provided the number of used licenses for the relevant equipment type has not reached the limit of allowed devices.
Cut Through	Opens a Telnet session to the selected device. Applicable only to devices that support this feature. (BreezeMAX SUs do not support Telnet.) Not available if more than one device is selected or if the State is other than Up.

Parameter	Description
Multiple Configuration	Opens the Multiple Configuration window, allowing simultaneous configuration of several selected devices. The Multiple Configuration option is applicable only if the Device Driver for the relevant devices supports the Multiple Configuration capability. Available only if the State of all selected devices is Up. For more details, see the *Device Manager User Manual*.
Backup Configuration	Opens the Configuration Backup task, allowing to create and schedule a configuration backup task for the selected devices. Available only if the State of all selected devices is Up. See "BreezeMAX Configuration Backup Task" - Section 5.2.9. See also the "Backup Files Manager" - Section 3.5.
Export to CSV	Exports the general information of selected devices to an external Comma Separated Value (CSV) file. Click to export, browse to the desired location, enter a file name, and click **Save**. The information displayed for each device in the Equipment Manager is exported.
Open Map	Opens the location Map, displaying the selected map for the applicable Location. Available only when a location is assigned to the selected device. Not available if more than one device is selected or the device's State is other than Up. For more details, refer to "Location Manager" - Section 3.3

3.2.1 Filtering the List of Devices

In addition to the *Criteria* scheme that enables to filter the displayed devices (see Section 1.7.5.1), the Equipment Manager also provides a list of Type filters, which are most commonly used. These include: BreezeMAX BS Equipment and BreezeMAX SU Equipment.

3.2.2 The Equipment Editor

The Equipment Editor enables to edit general information pertaining to the selected device.

To open the Equipment Editor:

From the *Equipment Manager*, select a Base Station/SU from the list and click **Edit**. The Equipment Editor window is displayed for the selected device. When selecting multiple devices, only Location and Contact can be edited simultaneously for all selected devices.

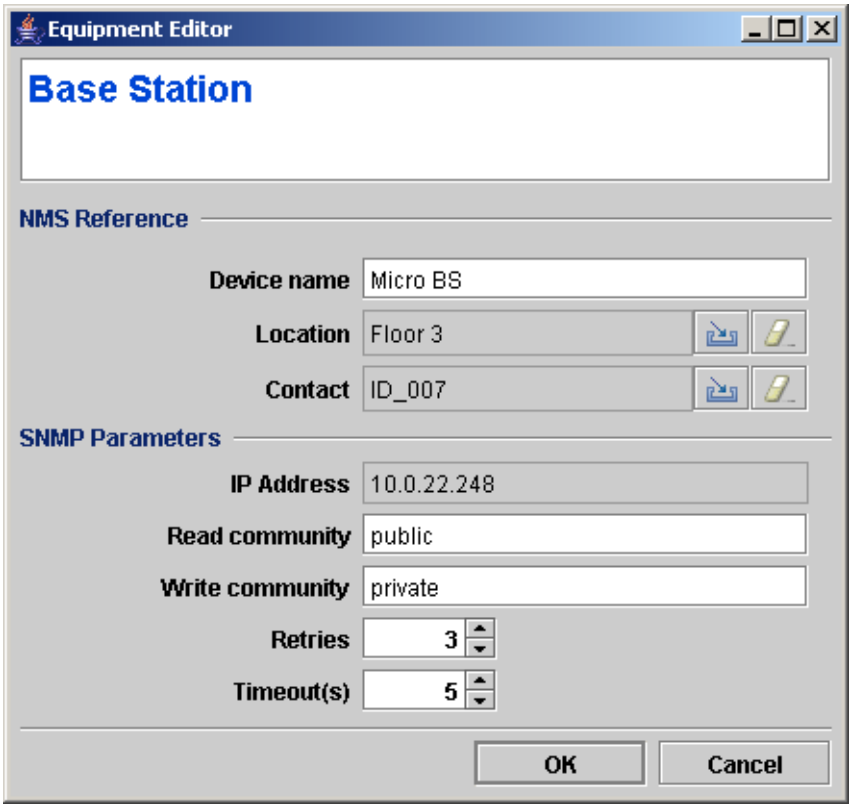

Figure 3-4: Equipment Editor

The Equipment Editor includes the following fields:

Parameter	Description
NMS Reference	
Device Name	The device's name in the NMS. By default, this is the name configured in the device, but it can be edited. The Device Name of an SU cannot be edited.
Location	The device's location. Click on the Browse icon to open the Select Location window and select a location. Click the Eraser icon to clear the Location field.
Contact	The contact associated with the device. Click on the Browse icon to open the Select Contact window and select a contact. Click the Eraser icon to clear the Contact field.
SNMP Parameters (Not applicable for SUs)	
IP Address	A read-only display of the device's IP Address.

Parameter	Description
Read community	The Read community string (password) for SNMP get operations. This string is used by the SNMP agent to allow/disallow SNMP read access. The Read default value is *public*.
Write community	The Write community string (password) for SNMP set operations. This string is used by the SNMP agent to allow/disallow SNMP write access. The Write community can also be used for read (get) operations. The Write default value is *private*.
Retries	The maximum number of retries for SNMP/TFTP communication with the Device. The range is from 0 to 255. The default is 2 retries.
Timeout(s)	The maximum time in seconds that the requesting process waits for a response from the Device before attempting a retransmission (or aborting if the maximum number of retries has been reached). The available range is 1 to 3600 seconds. The default is 5 seconds.

NOTE

For SUs, only Location and Contact can be edited.

3.3 Location Manager

The Location Manager enables to specify information regarding the physical location of equipment managed by AlvariSTAR, to facilitate quick detection of managed objects and to help drill down quickly when using maps to view specific equipment components.

You can specify equipment locations within the Location Manager. Note that a location can have a “Parent” Location, meaning that it belongs to a subset of another location. For example, if network objects are on the third floor of a facility, you can designate both the building and the specific floor as locations; the building would be the parent of the floor. You may define multiple levels for locations. In the current example, the city in which the building is located can be defined as the parent location of the building, and so on.

To associate a single device with a location or several devices with a single location, open the Equipment Editor for the device(s), click the **Browse** button next to the Location field to open the Select Location window and select a location. For further details, refer to Section 3.2.2.

To open the Location Manager:

Select *Inventory* > *Location Manager* from the *File* > *Open* > *AlvariSTAR* menu or the Navigation Pane. The Location Manager window is displayed.

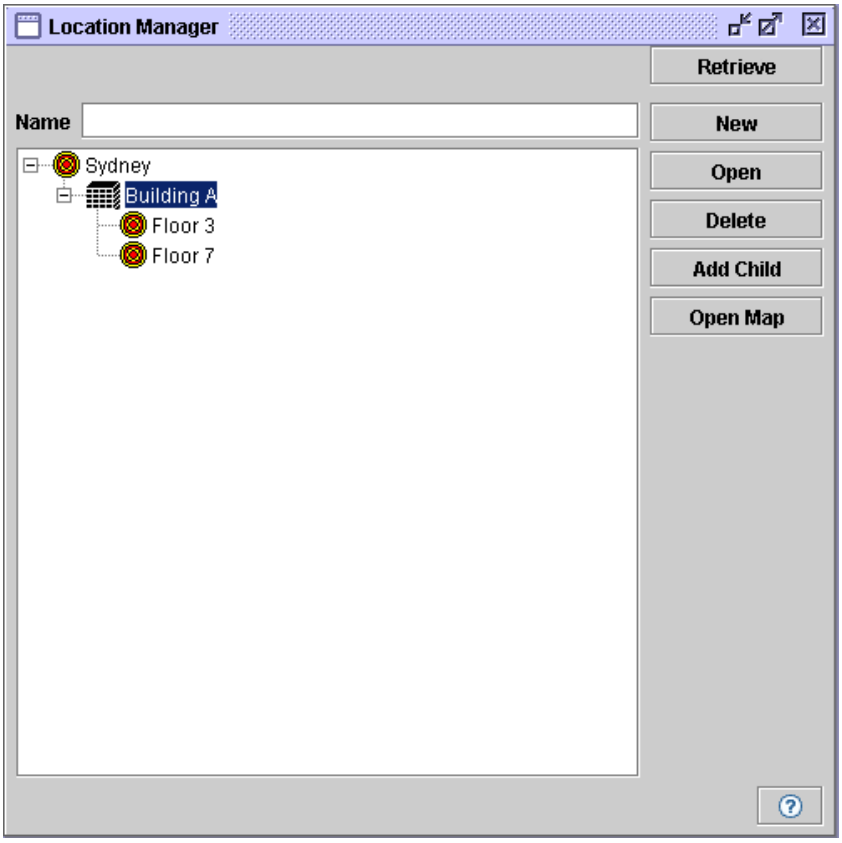

Figure 3-5: Location Manager

You can select one or more locations from the list.

The following command buttons are available in the Location Manager:

Parameter	Description
New	Opens the Location Editor, through which you can define a new location. Refer to Section 3.3.2, for more information
Open	Opens a Location Editor for a selected location, enabling you to modify the definition of the Location. See Section 3.3.2 for more information.
Delete	Enables to delete the selected location(s). When deleting a parent location, the application also deletes its associated child locations. A location associated with equipment cannot be deleted.
Add Child	Opens the Location Editor, through which you can define a new child location that will be subordinate to the selected location. When creating a child location, the name of the parent location field is displayed in the Parent field.

Parameter	Description
Open Map	Opens the Location Map, displaying the selected location. See Section 3.3.4 for more information.

3.3.1 Searching for a Location

To search for a specific location, enter the full name of the location (California, for example) or part of the name (Ca) in the *Name* field. Only locations matching that specification appear. Note that the filter is case-sensitive and the results are displayed immediately.

3.3.2 Location Editor

The Location Editor enables to create a new location or modify details of an existing location.

To create/modify a location:

1 In the Location Manager, click **New** to create a new location, or, to edit an existing location, select a location from the list and click **Open** or double-click on the selected location. The Location Editor is displayed.

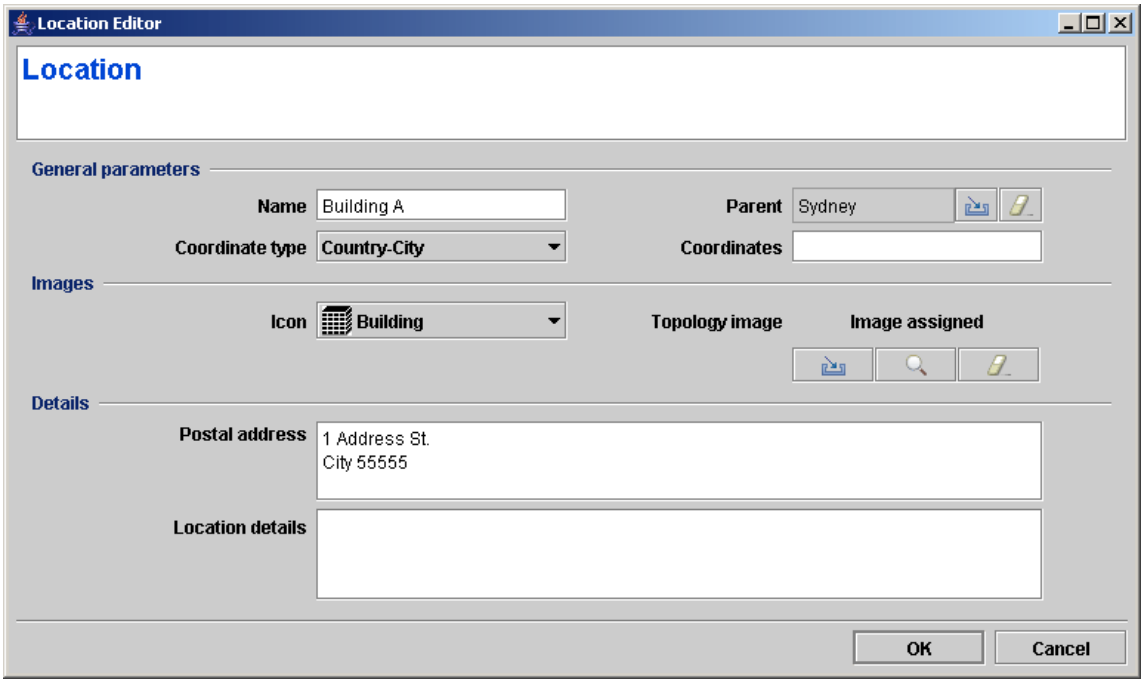

Figure 3-6: Location Editor

The Location Editor includes the following fields:

Parameter	Description
General parameters	
Name	Enter a unique name for the Location, up to 32 printable characters. This is the name that will be used for searching.
Parent	The parent of this location (the location to which this location is subordinate). Click the **Browser** button to open the *Select Location* window through which you can select a Parent Location. Click the **Eraser** icon to clear the Parent Location field.
Coordinate Type	Specifies the way coordinates are designated; see Section 3.3.3 for more information. Valid types are: Country-City, Latitude-Logitude, Area Code-prefix, Vertical-Horizontal.
Coordinates	The coordinates of the location, using the Coordinate Type specified above. Up to 80 printable characters.

NOTE

Coordinates do not relocate icons in geographic topology maps; dragging icons does.

Images	
Icon	Select an icon from the drop-down list to associate it with the location. Available icons are: Building, Location.
Topology Image	Click the **Browse** button to open the *Select Location* window through which you can select a map and associate it with the location. Click the **Eraser** icon to clear the field. Click the **Preview** button to view the associated map. Depending on whether or not an image is assigned, the label changes from "No image assigned" to "Image assigned".
Details	
Postal Address	An optional field for entering the address of the location. A string of up to 80 characters.
Location Details	An optional field for entering a description of the location. A string of up to 80 characters.

2 Type in or modify the fields as required.

3 Click **Apply**.

3.3.3 Coordinate Types

You can define locations using a variety of coordinate types, enabling accurate definition of locations. The following are the default coordinate types:

Parameter	Description
Country-City	Country and city access codes. Example: 049-071
Latitude-Longitude	Latitude and longitude. Example: 38.57N, 121.47W
Area Code-Prefix	Area code and prefix. Example: 916-939
Vertical-Horizontal	Vertical / horizontal coordinates, developed by Bell Systems.

NOTE

Coordinates type and coordinates values are not used for displaying the location in geographic topology. They are available for informational purposes only.

3.3.4 Location Map

The Location Map viewer displays a topology view of network devices and their relationships. Clicking on the **Open Map** button opens the Location Map viewer for the selected location, displaying its sub-locations and the equipment associated with it. Associating a map with a location is optional; if no map is associated with the location, the Location Map viewer will be empty. Each location can either share a map with any other location or it can be associated with its own map.

3.3.4.1 Defining Locations, Sub Locations and Maps

Primary (first level) locations have no parent locations. However, you can define sub-locations (second level) whose “parents” are the primary locations. You may continue and define third, fourth and fifth levels, where the parent location for level N is a location in level N-1.

For each location you can also define a Geographical Map.

To define locations, sub locations, and/or maps:

1 **Locations**: From the Location Manager, click **New** to open the Location Editor.

Sub Locations: Select a location and click **Add Child** to open the Location Editor with the selection location as the default parent location. Alternatively, click **New** to open the Location Editor and select an existing node as the parent in the Parent field.

2 Define the Location Name.

NOTE

For first level locations, the parent location field must be empty. For additional locations, a parent location must be defined.

3 If you want to associate the location with a map, select the required map in the Topology Image field.

NOTE

The required maps must be available (as *.jpg, *.gif, *.bmp, or *.png files) in the client station. The file size is limited to 512 kb.

4 You can optionally define the Location Type, Icon and other details available in the Location Editor.

5 You can associate equipment with locations. See Section 3.2.2.

3.3.4.2 Location Map Viewer Options

The Location Map viewer includes the following controls:

Parameter	Description
Up one level	Opens the next higher level of the topology map in the same window. Disabled with in first level locations.
Display BreezeMAX SU	Check to display the associated SUs on the map. Only SUs associated with the relevant location are displayed. If the serving Base Station(s) are associated with the same location, each of the displayed SU will be connected to the serving device.
Save	Saves the changes made to the map.
Cancel	Closes the Location Map viewer without saving.

The Location Map viewer provides a pop-up menu with the following options when right-clicking on an equipment/location icon:

Parameter	Description
Drill down	Opens the next lower level of the topology map in the same window. Available only when right-clicking a location in the map, provided there is a sub-location.
Up one level	Opens the next higher level of the topology map in the same window. Disabled for first level locations.
Configure	Available only for equipment. Opens the Configuration window, enabling to configure the selected device. You can also double-click on the device icon on the map. Refer to the *Device Manager User Manual*.
Cut Through	Available only for equipment. Opens a Telnet session to the device. Applicable only for devices that support this feature. (SUs do not support Telnet.)
Open Alarms	Available only for equipment. Opens the Event Monitor window, enabling to view the alarms (if any) associated with the selected device.

The background color of the device's icon on the map is in accordance with the device's alarm status (the highest severity open alarms). For more information, refer to "Alarm Severities" - Section 6.4.2.

Place a cursor on an icon to view its general details.

3.4 Contact Manager

The Contact Manager enables to organize and manage your contacts. Each device can be associated with a contact.

To open the Contact Manager:

1 Select *Inventory* > *Contact Manager* from the *File* > *Open* > *AlvariSTAR* menu or the Navigation Pane. The Contact Manager displays a list of available contacts.

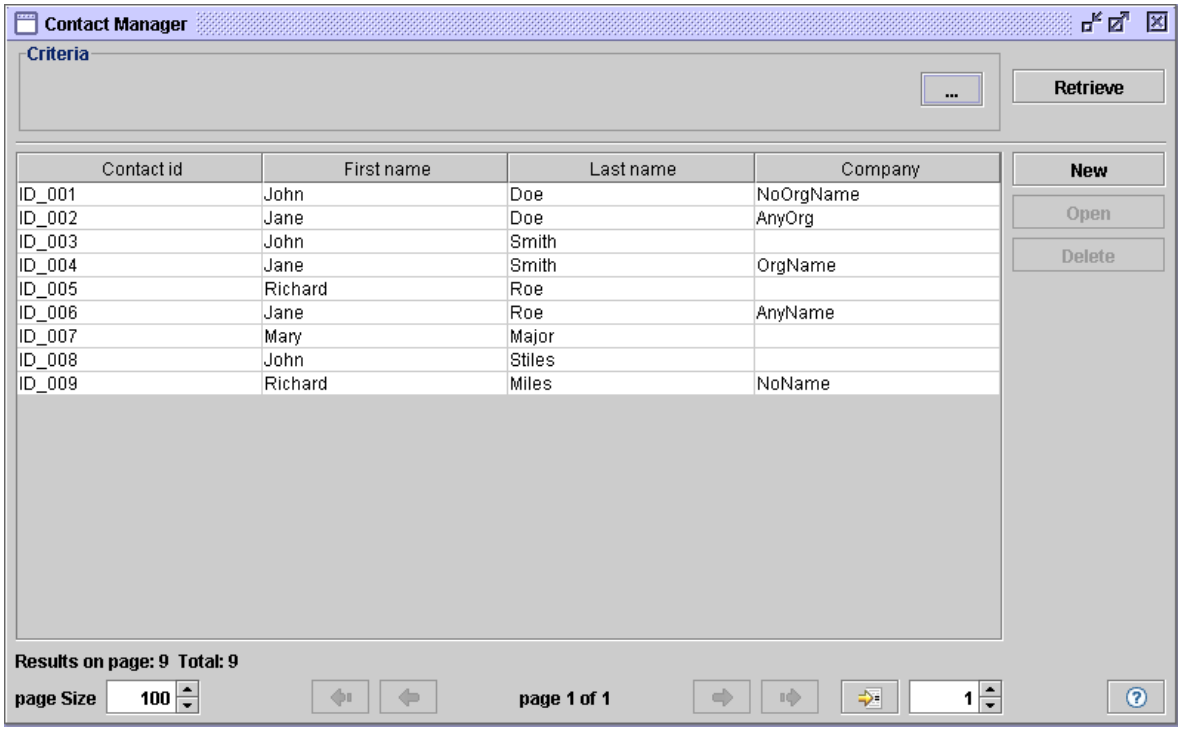

Figure 3-7: Contact Manager

2 Click **Retrieve** when the Contact Manager window initially opens to display all defined contacts. You can filter the display by selecting one of the predefined filters in the *Criteria* browser and then clicking on **Retrieve**.

The following are the controls on the Contact Manager window:

Parameter	Description
New	Opens the *Contact Editor* window, enabling to create new contacts.

Parameter	Description
Open	Opens the *Contact Editor* window, enabling to modify the selected contact.
Delete	Deletes the selected contact(s) from the Contact Manager window and from the database.

3.4.1 Associating Devices with a Contact

To associate devices with a contact:

Open the Equipment Editor of the device. Click the **Browse** button next to the Contact field to open the *Select Contact* window and select a contact.

3.4.2 Creating or Modifying a Contact

To create/modify a contact:

1 From the Contact Manager window, click **New** to create a new contact. To modify an existing Contact, select a contact from the list and click **Open**, or double-click on the selected contact.

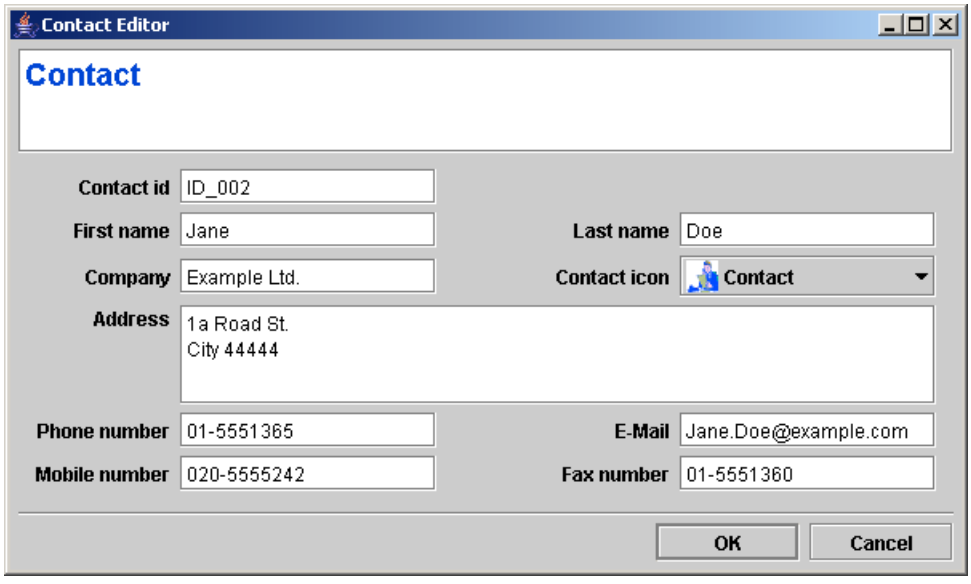

Figure 3-8: Editing Contact Window

2 Configure the following parameters:

Parameter	Description
Contact ID	A unique identifier for this contact. Up to 80 printable characters.
First Name	Optional. The contact's first name. Up to 80 printable characters.
Last Name	Optional. The contact's last name. Up to 80 printable characters.
Company	Optional. The contact's company name. Up to 80 printable characters.
Contact Icon	Optional. Select from the drop-down list an icon to represent this contact: Contact/Group.
Address	Optional. The contact's address. Up to 80 printable characters.
Phone Number	Optional. The contact's phone number. Up to 80 printable characters.
Mobile Number	Optional. The contact's mobile number. Up to 80 printable characters.
Email	Optional. The contact's e-mail address. Up to 80 printable characters.
Fax Number	Optional. The contact's fax number. Up to 80 printable characters.

3 Click **OK**, to save and close the contact, or click **Cancel** to close the window without saving the changes.

4 To display the new contact in the Contact Manager, click **Retrieve**.

3.5 Backup Files Manager

The Backup Files Manager displays all backup configuration files available for restoring. It also enables to export configuration backup files to the client file-system and to import configuration backup files stored in the client file-system. By default, the system keeps up to three backup files per network element.

To open the Backup Files Manager

1 Select *Inventory* > *Backup Files Manager* from the *File* > *Open* > *AlvariSTAR* menu or the Navigation Pane. The Backup Files Manager displays a list of available configuration backup files.

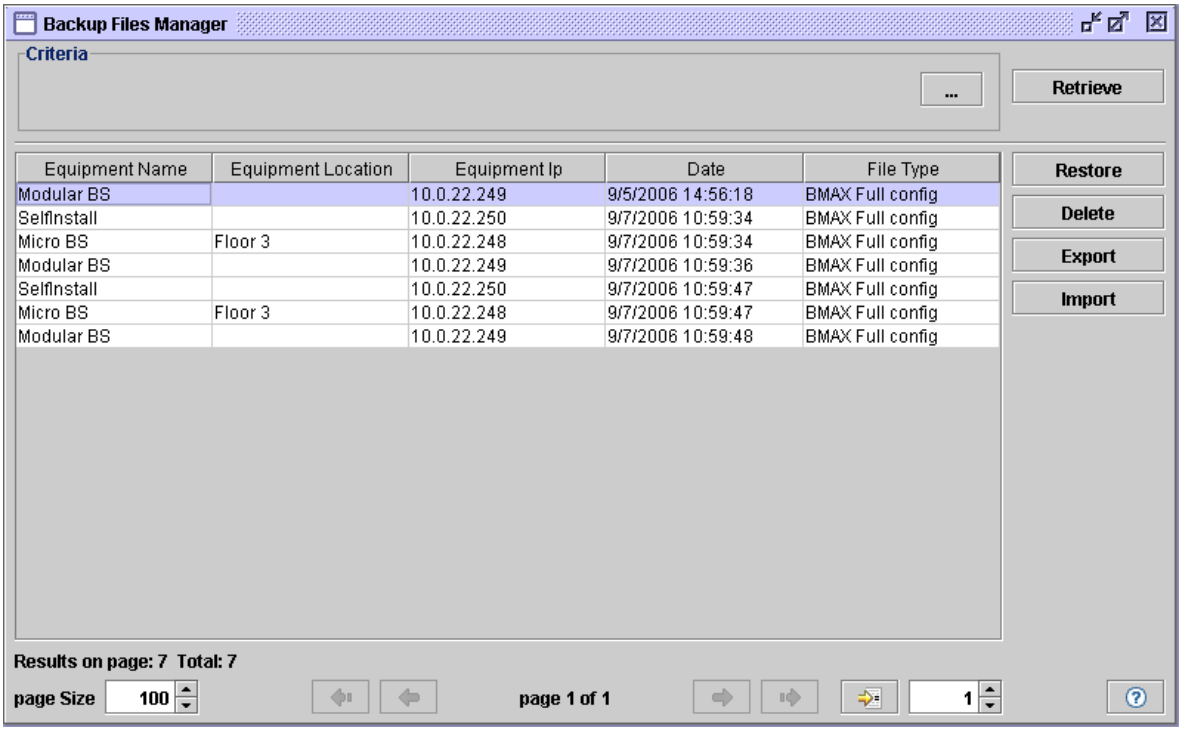

Figure 3-9: Backup Files Manager

2 Click **Retrieve** when the Backup Files Manager window initially opens to display all available backup files. You can filter the display by selecting one of the predefined filters in the *Criteria* browser and then clicking on **Retrieve**.

The following are the controls on the Backup Files Manager window:

Parameter	Description
Restore	Opens the Restore Configuration task window, enabling to select the equipment to which the backup file is to be loaded and to run the task. See Section 3.5.1. Not available if more than one backup file is selected.
Delete	Deletes the configuration backup file from the database. Select the file(s) to remove and click **Delete**.
Export	Exports the configuration backup file to the client file-system. Click to export, browse to the desired location on the client file-system, enter a name for the file, and click **Save**. Not available if more than one row is selected.
Import	Imports a configuration backup file from the client file-system. Click to import, browse to the location on the client file-system where the file is stored, select the file and click **Open**.

3.5.1 Restore Configuration Task

The Restore Configuration Task window enables to load a selected backup file to selected equipment.

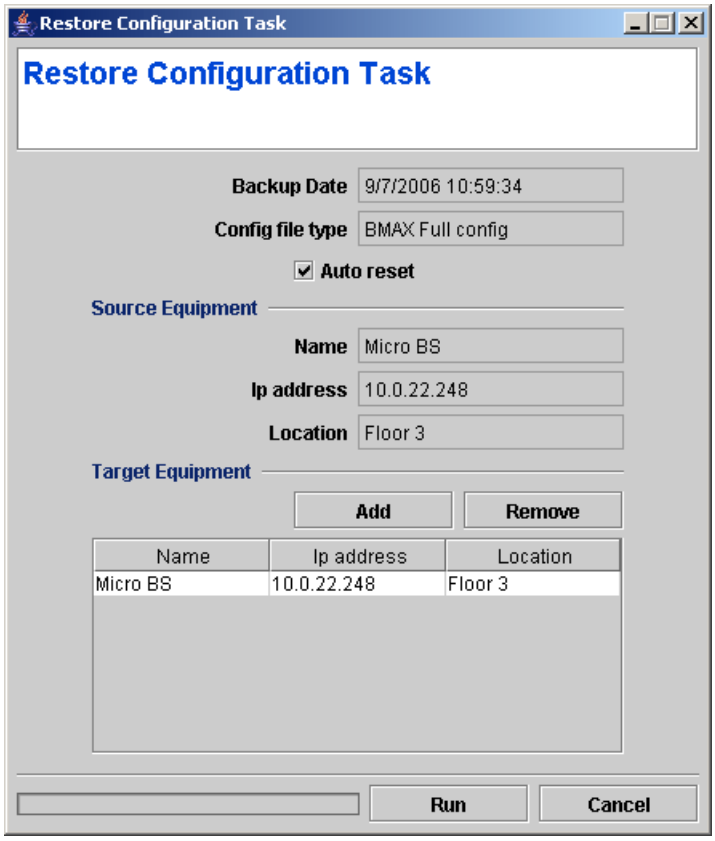

Figure 3-10: Restore Configuration Task Window

The Restore Configuration Task window includes the following fields:

Parameter	Description
Backup Date	A read-only display of the date and time in which the backup file was created.
Config File Type	A read-only display of the type of backup file created: *Full config*, *Service Profile*, *Services*, *Traps*, *Filters*. See Section 5.2.9 for details on each type.
Auto Reset	Check to automatically reset the units after loading the configuration backup file.
Source Equipment	
Name	A read-only display of the name of the equipment from which the configuration backup file was created (the source equipment).
IP Address	A read-only display of the IP address of the source equipment.
Location	A read-only display of the location associated with the source equipment.

You can apply a specific configuration to selected equipment by adding them to the list of Target Equipment. By default, the source equipment, i.e., the equipment from which the configuration backup file was created, is listed in the Target Equipment area. You can remove it from the list and/or add other equipment to the list.

To restore the selected configuration backup file:

1. In the *Restore Configuration Task* window, click **Add**. The *Select Equipment* window opens.
2. Select the equipment to undergo configuration restoring and click **Select**. The selected equipment is listed in the Target Equipment list. You can use the Delete button to remove equipment from the list.
3. Click **Run**. If Auto reset was selected, a confirmation message appears warning you that the selected units will automatically reset after configuration is restored.
4. Click **OK** to confirm. The *Runtime Results* window opens, displaying the task's progress and results. Click **Close** to close the *Runtime Results* window.
5. In the *Restore Configuration Task* window, click **Cancel** to close the window.

3.6 PM Collection Viewer

After the required data has been collected (via the Performance Collection task, see Section 5.2.7) and stored in the database, the Performance Viewer can be used to provide performance tracking by displaying graphs of selected counters. Collected data may also be exported as Comma Separated Values (csv) files.

From the Performance Viewer you can:

- View the current status of data collection tasks
- Access the Graph window for viewing graphs of collected data for selected counters (see Section 3.6.1)
- Export collected data as Comma Separated Values (csv) files (see Section 3.6.2).

To open the Performance Viewer:

Select *Inventory* > *PM Collection Viewer* from the *File* > *Open* > *AlvariSTAR* menu or the Navigation Pane. The *Performance Viewer* is displayed:

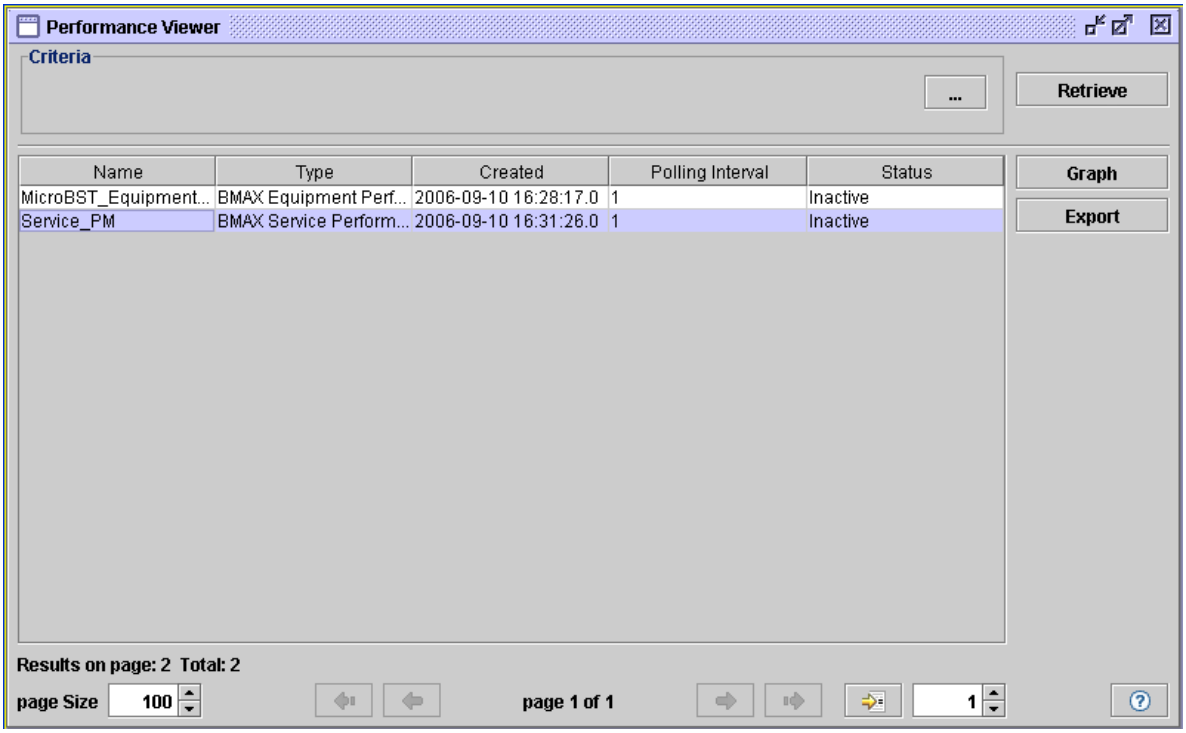

Figure 3-11: Performance Viewer

The performance viewer displays the following information for each polling session:

Parameter	Description
Name	The name of the performance collection task, as defined in the Task Manager.
Type	The type of task, as defined in the Task Manager: Service Performance, Equipment Performance
Polling Interval	The time (in minutes) between polls.
Created	The date and time in which the performance task was created.
Status	The status of the task: Active (the task is currently running) / Inactive (the task is idle).

The Performance Viewer includes the following controls, which are activated upon selection of a performance collection task from the list:

Parameter	Description
Graph	Opens the Graph Generator window, enabling to build a graph from the collected data, according to user specifications. See Section 3.6.1.
Export	Opens the Export PM Collection Data window for the selected task, enabling to export the collected data to a CSV file. See Section 3.6.2.

3.6.1 The Graph Generator

To build a graph for the selected performance collection task:

1. In the Performance Viewer, select a task from the list. The Graph button becomes active.
2. Click on **Graph**. The graph generator opens.

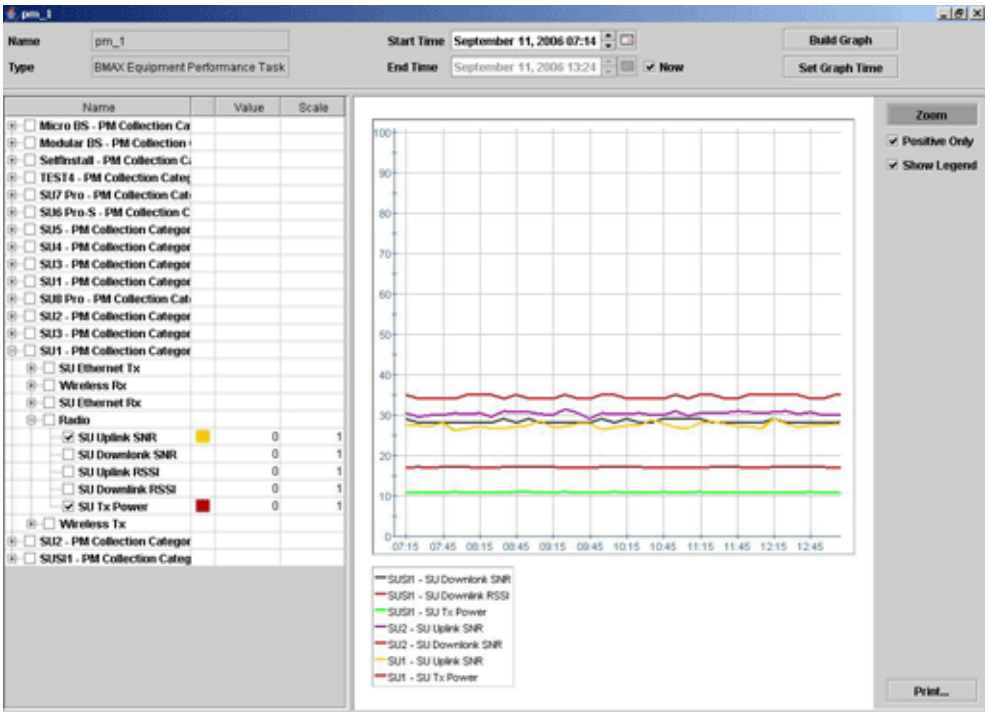

Figure 3-12: Graph Generator

The Graph Generator page comprises three sections: the graph generation controls at the top, the counters selection section on the left and the graph and control buttons section on the right. For convenient viewing of the

required information, you can change the relative sizes of the counters selection section and graph section, by dragging the line separating them.

3 In the *Start/End Time* fields, select the date and time range from which the data is to be displayed in the graph. You can highlight the value to change (month, day, year) and click on the up/down arrows to change the value, or alternatively, you can pick a specific date using the calendar icon. For End Time, you can also check the **Now** box, to define the time range until the present time.

4 The counters selection table, on the left side of the window, displays all the devices/services belonging to the selected PM collection task. Select the equipment/service and specific counters to display in the graph. For more information on the counters selection section, see Section 3.6.1.1.

5 Click the **Build Graph** button.

You can change the graph to display only a specific timeframe.

To set the graph's timeframe:

Select the *Start Time* and *End Time* in their respective fields and click **Set Graph Time**.

3.6.1.1 The Counters Selection Section

The counters selection section enables to select specific counters, to define the polling interval for the on-line display and to define the graph's values scale for each of the selected counters.

The counters selection section, on the left side of the window, displays all the counters groups applicable to the relevant device.

You can perform the following operations in the Counters Selection section:

To expand/collapse the list of counters:

1 Use the Expand/Collapse (+/-) check-box on the left side of the device's name to view/hide all counters groups available for the device.

2 Use the Expand/Collapse (+/-) check-box on the left side of the counters group name, to view/hide all counters available in the group.

To the right of each counter, the following details are available:

- The color of the graph for this counter (available only for a selected counter)
- The scale value for the graph (see details below)

To view the graph of a counter:

Select the check box to the left of a counter to add it to the graph and view its details. The color to be used in the graph for the selected counters is displayed to the right of the counter.

To change the color of a counter's graph:

Click on the color display (on the right side of the selected counter). The **Pick a Color** window opens, allowing you to change the color's properties.

Deselect the check box to terminate the on-line display of the counter. Select again to continue the display.

NOTE

You can also select/deslect all the counters in a group or all counters in the relevant device by using the relevant check box(s).

To optimize the value (vertical) axis of a counter:

The values scale (vertical axis) is fixed, between -100 to +100 (or between 0 to 100 for a Positive Only graph). Some counters may have values that either exceed this range or are too small. The value scale of each counter is displayed to the right of the counter's name (the default is 1.0). To change the value scale of a counter, select it and choose the desired scale from the scale drop-down list that will be displayed on the right side of the counter. The values displayed for this counter on the graph are the actual counter values multiplied by the scale factor.

3.6.1.2 The Graph and Controls Section

The graph and controls section contains the graph area, used for displaying the selected counters over time.

The names and details of the counters that were selected are displayed below or to the left of the graph area.

The following graph controls are available:

- **Pan/Zoom** Button**:** Toggles between the **Pan** and **Zoom** modes.
- **Positive Only** Check Box**:** Select to set the boundaries of the values (vertical) axis between 0 and +100. Deselect (the default) to set the boundaries between -100 to +100.
- **Print...:** Enables to setup the page, print the graph or display a print preview.

You can use the **Pan/Zoom** toggle button to either shift the time axis or change its resolution:

To shift the time axis:

1. Make sure that *Pan* mode is selected. If *Zoom* mode is selected, click the button to toggle to *Pan* mode.
2. Drag the graph surface left or right to shift the displayed section of the Time axis.

To change the resolution of the time axis:

1. Make sure that *Zoom* mode is selected. If *Pan* mode is selected, click on the button to toggle to *Zoom* mode.
2. Drag the graph surface left or right to change the resolution of the Time axis.

To print or preview a graph:

Click on **Print...**. A pop-up menu opens with three options:

- **Print...:** To open the Print dialog box for selecting a printer, setting up the printing properties and printing the graph.
- **Print Preview...:** Displays a preview of the graph before printing.
- **Page Setup...:** To open the Page Setupo dialog box

3.6.2 Exporting Collected Data

To export collected data:

1. In the Performance Viewer, select a task from the list. The Export button becomes active.
2. Click on **Export**. The Export PM Collection Data window for the selected task opens.

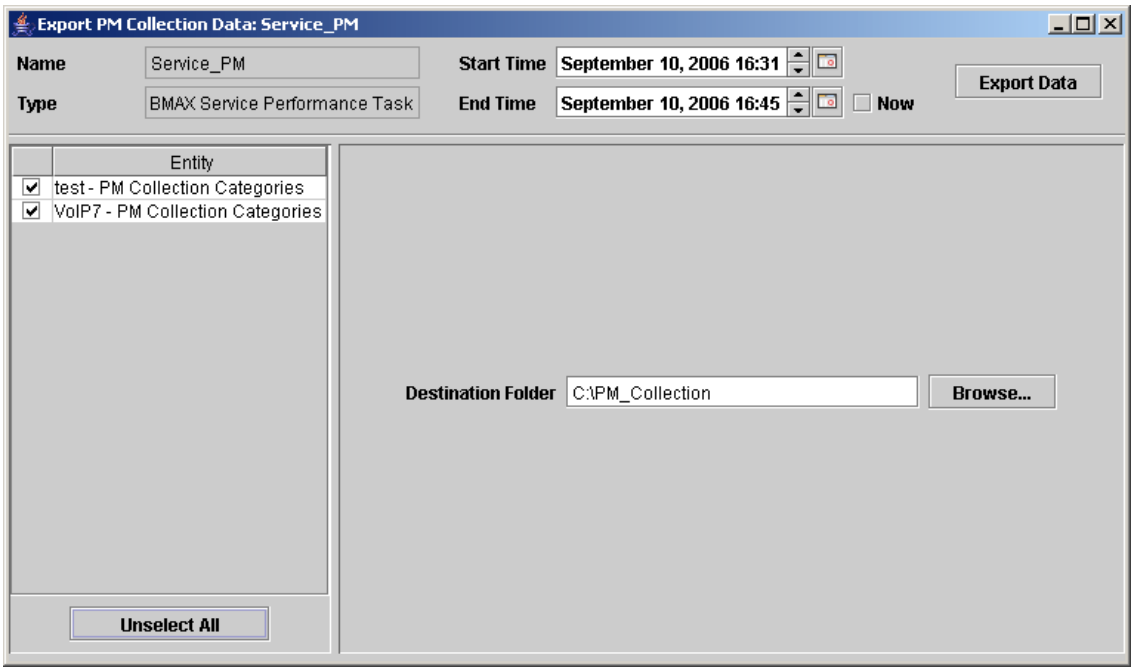

Figure 3-13: Export PM Collection Data Window

3. In the *Start/End Time* fields, select the date and time range from which the data is to be exported. You can highlight the value to change (month, day, year) and click on the up/down arrows to change the value, or alternatively, you can pick a specific date using the calendar icon. For End Time, you can also check the **Now** box, to define the time range until the present time.
4. Select the required equipment/services from the list of entities. Check the box next to the name of the device, or click on **Select All** to select all the listed entities (the button changes to *Unselect All*, enabling to unselect all entities).
5. In the *Export File* field, click on the **Browse** button to select a location on the client file system where you want to save the exported file and click **Select**.

6 Click on the **Export Data** button. A separate CSV file is saved in the selected location on the file system for each selected equipment/service.

The *Export PM Collection Data* window displays the name and type of task, as defined in the Task Manager.

4

Chapter 4 - Provisioning

In This Chapter:

- "Introduction to Provisioning" on page 90
- "Service Manager" on page 91
- "Service Profile Manager" on page 95
- "Subscriber Manager" on page 113

4.1 Introduction to Provisioning

The Provisioning module provides the tools to view and manage Services and related entities (Subscribers and Service Profiles) in the entire network.

A Service is a virtual connection between a Subscriber's application and the Network Resource. The Network Resource could be Internet, Content Provider, Corporate Network, etc.

A Subscriber is an entity that may be associated with any number of devices connected to any number of SUs. Each Service associates a certain Service Profile with Subscriber's device(s) behind a specific SU. The Service Profile's properties depend on the Service Type.

The Provisioning module includes the following managers:

- "Service Manager" on page 91
- "Service Profile Manager" on page 95
- "Subscriber Manager" on page 113

4.2 Service Manager

The Service Manager provides a comprehensive view of the current services defined in the entire managed network. From the Service Manager you can:

- View currently defined services that exist in the database, according to various selection criteria
- View general information on the displayed services
- Open the Subscriber Editor for the Subscriber associated with a selected Service
- Create a new service.
- Access the Graph window for viewing the graph of collected data for a selected service. This function is only available for services whose operational status is Up.

To open the Service Manager:

Select *Provisioning* > *Service Manager* from the *File* > *Open* > *AlvariSTAR* menu or in the Navigation Pane. The Service Manager window opens, with the default display of Services that exist in the device and in the database. The background color of the service's icon is in accordance with the service's operational status: green indicates that the service is Up; red indicates that the service is Down.

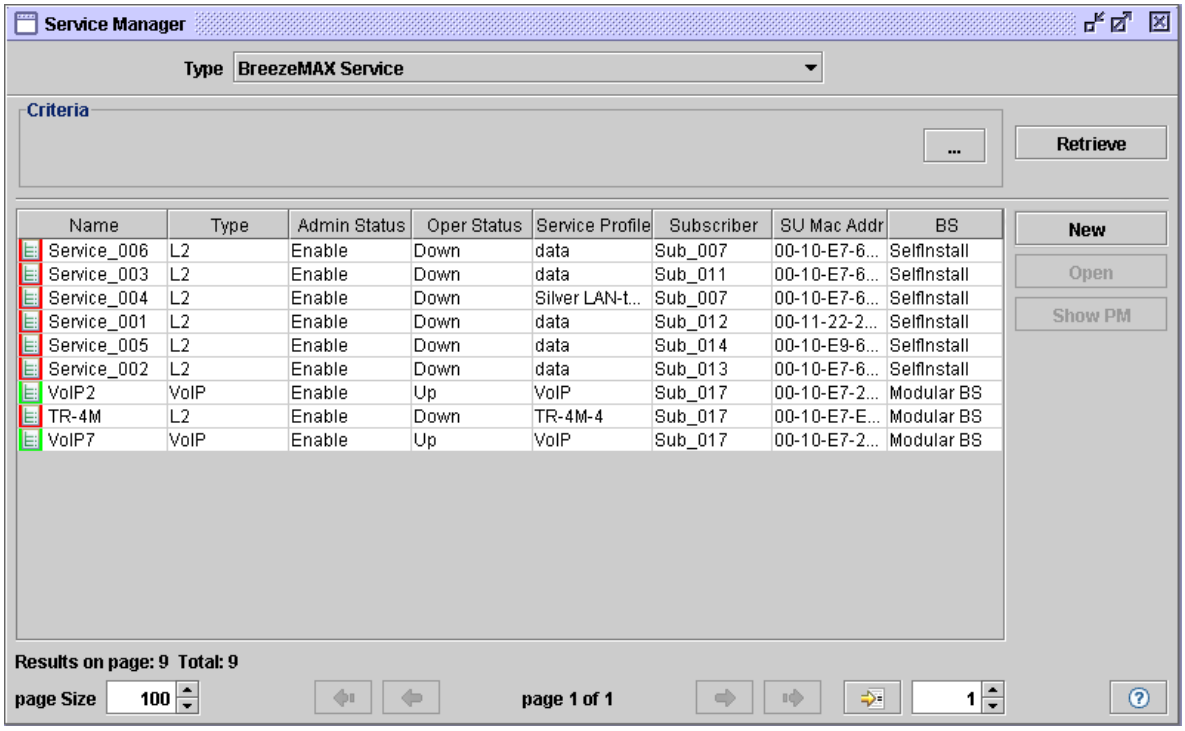
Service Manager
Type BreezeMAX Service
Criteria
...
Retrieve
Name Type Admin Status Oper Status Service Profile Subscriber SU Mac Addr BS
Service_006 L2 Enable Down data Sub_007 00-10-E7-6... SelfInstall
Service_003 L2 Enable Down data Sub_011 00-10-E7-6... SelfInstall
Service_004 L2 Enable Down Silver LAN-t... Sub_007 00-10-E7-6... SelfInstall
Service_001 L2 Enable Down data Sub_012 00-11-22-2... SelfInstall
Service_005 L2 Enable Down data Sub_014 00-10-E9-6... SelfInstall
Service_002 L2 Enable Down data Sub_013 00-10-E7-6... SelfInstall
VoIP2 VoIP Enable Up VoIP Sub_017 00-10-E7-2... Modular BS
TR-4M L2 Enable Down TR-4M-4 Sub_017 00-10-E7-E... Modular BS
VoIP7 VoIP Enable Up VoIP Sub_017 00-10-E7-2... Modular BS
New
Open
Show PM
Results on page: 9 Total: 9
page Size 100
page 1 of 1
1

Figure 4-1: Service Manager

To view Services according to preferred selection criteria:

1 Select the Device Family Services Type from the **Type** drop-down menu.

NOTE

In the current release, only BreezeMAX Services are supported.

2 Click on the **Select Filters** button to narrow the search criteria. See Section 1.7.5.1 for information on using filters.

3 Click on the **Retrieve** button to view the Services that match the selection criteria.

The Services table displays the following details for each of the applicable Services:

Parameter	Description
Name	The Service Name.
Type	The Service Type: L2, PPPoE or VoIP.
Admin Status	The administrative status of the Service: Enable/Disable.
Oper Status	The operational status of the Service. Up means that the Service is currently in use.
Service Profile	The Name of the Service Profile used in the Service.
Subscriber	The ID (Name) of the Subscriber to which the Service is allocated.
SU Mac Addr	The MAC Address of the SU associated with the Service.
BS	The IP of the Base Station/Micro Base Station providing the Service.

To open the Subscriber Editor for the Subscriber associated with a selected Service:

Use any of the following options to open the Subscriber Editor for the Subscriber associated with a selected Service (see Section 4.4.2.2):

- Double-click on a selected entry in the Services table, or:
- Select an entry and click on the **Open** button on the right side of the window, or:
- Right-click on a selected entry to open the option selection box, and then click on the **Open** option.

To create a new service:

The Service Manager enables to easily create a new service.

1. In the Service Manager, click on **New**. The *Select subscriber* window opens.
2. Select a subscriber from the list and click **Select**. The *Select subscriber* window closes and the *Select equipment* window opens.
3. Select the equipment from the list and click **Select**. The *Select equipment* window closes and the *Subscriber Editor* opens.
4. Enter a unique name for the new service and fill in all the required parameters. When done, click **Apply**.

5 In the Service Manager, click **Retrieve** to view the newly added service in the list.

For further details on services, refer to the *BreezeMAX Device Manager User Manual*.

To display the performance monitoring graph for a service:

In the Service Manager, select a service from the list and click **Show PM**. You can view the performance monitoring graph only for a selected service whose operational status is Up. For more detailed information on the Graph's components, see the *Device Manager User Manual*.

4.3 Service Profile Manager

"The Service Profile Manager Window" - Section 4.3.1

"The Service Profile Editor" - Section 4.3.2

"The Service Profile Distribution Task" - Section 4.3.3

4.3.1 The Service Profile Manager Window

The Service Profile Manager window provides a comprehensive view of the current Service Profiles defined in the entire network. This includes Service Profiles that are defined in managed devices (deployed), and Service Profiles that are defined only in the data base (undeployed). From the Service Profile Manager window you can:

- View currently defined Service Profiles that exist in the database, according to various selection criteria
- Delete Service Profiles from the database. Services that are deployed cannot be deleted.
- Open the Service Profile Editor for editing an existing Service Profile or creating a new one, and for deploying/undeploying Service Profiles in selected Base Stations.

To open the Service Profile Manager:

Select *Provisioning* > *Service Profile Manager* from the *File* > *Open* > *AlvariSTAR* menu or in the Navigation Pane.The Service Profile Manager window opens, with the default display of all Service Profiles that exist in the database.

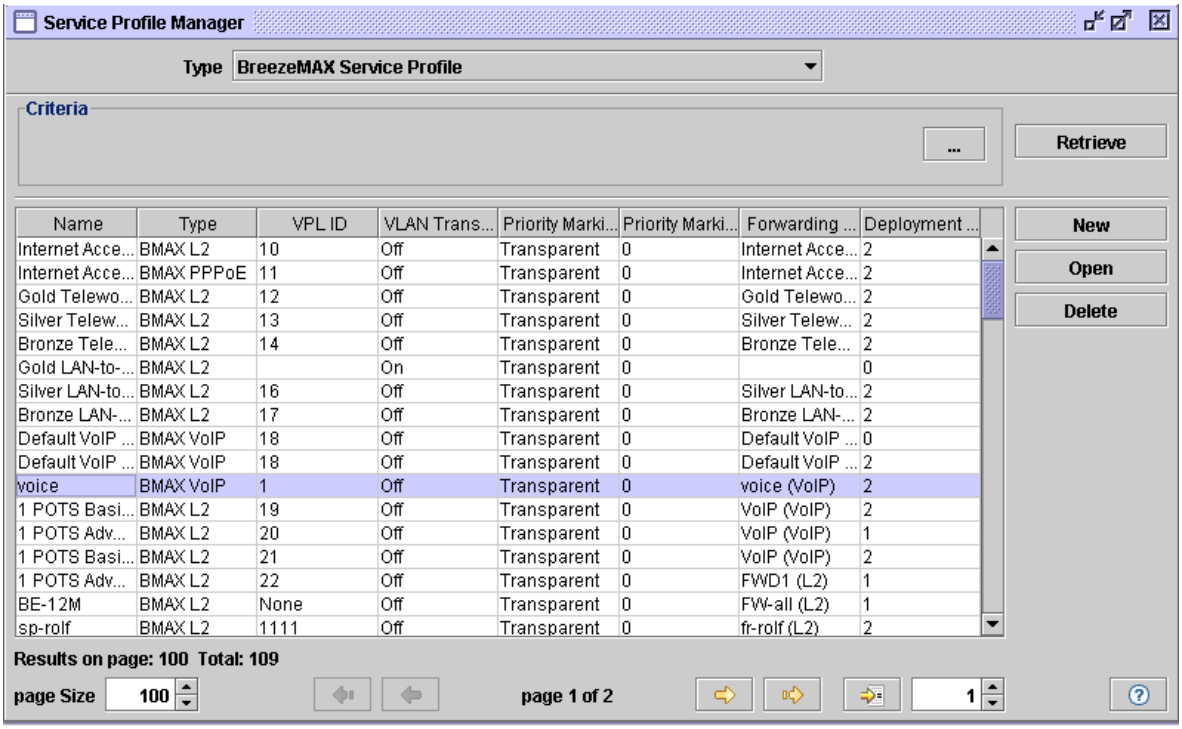
Service Profile Manager
Type
BreezeMAX Service Profile
Criteria
...
Retrieve
Name
Type
VPL ID
VLAN Trans...
Priority Marki...
Priority Marki...
Forwarding ...
Deployment ...
Internet Acce... BMAX L2 10 Off Transparent 0 Internet Acce... 2
Internet Acce... BMAX PPPoE 11 Off Transparent 0 Internet Acce... 2
Gold Telewo... BMAX L2 12 Off Transparent 0 Gold Telewo... 2
Silver Telew... BMAX L2 13 Off Transparent 0 Silver Telew... 2
Bronze Tele... BMAX L2 14 Off Transparent 0 Bronze Tele... 2
Gold LAN-to-... BMAX L2 On Transparent 0 0
Silver LAN-to... BMAX L2 16 Off Transparent 0 Silver LAN-to... 2
Bronze LAN-... BMAX L2 17 Off Transparent 0 Bronze LAN-... 2
Default VoIP ... BMAX VoIP 18 Off Transparent 0 Default VoIP ... 0
Default VoIP ... BMAX VoIP 18 Off Transparent 0 Default VoIP ... 2
voice BMAX VoIP 1 Off Transparent 0 voice (VoIP) 2
1 POTS Basi... BMAX L2 19 Off Transparent 0 VoIP (VoIP) 2
1 POTS Adv... BMAX L2 20 Off Transparent 0 VoIP (VoIP) 1
1 POTS Basi... BMAX L2 21 Off Transparent 0 VoIP (VoIP) 2
1 POTS Adv... BMAX L2 22 Off Transparent 0 FWD1 (L2) 1
BE-12M BMAX L2 None Off Transparent 0 FW-all (L2) 1
sp-rolf BMAX L2 1111 Off Transparent 0 fr-rolf (L2) 2
New
Open
Delete
Results on page: 100 Total: 109
page Size
100
page 1 of 2
1

Figure 4-2: Service Profile Manager

To view Service Profiles according to preferred selection criteria:

1 Select the Device Family Services Profile Type from the **Type** drop-down menu.

NOTE

In the current release, only BreezeMAX Service Profiles are supported.

2 Click on the **Select Filters** button to narrow down the search criteria. See Section 1.7.5.1 for details on using filters.

3 Click on the **Retrieve** button to view the Service Profiles that match the selection criteria.

The Service Profiles table displays the following details for each of the applicable Service Profiles:

Parameter	Description
Name	The Service Profile Name

Parameter	Description
Type	The Service Profile Type: L2, PPPoE or VoIP.
VPL ID	The Virtual Private Link ID to be used in the backbone behind the Base Station. The VPL ID parameter is applicable only to Service Profiles with VLAN Transparency Off. Range: 0-4094, None or empty for Transparent Service Profiles.
VLAN Transparency	The VLAN Transparency defines the method of transferring packets to the operator's upstream network (On or Off). When set to On, data packets sent from the Base Station to the backbone will be transferred transparently. The VPL ID parameter is not applicable to Service Profiles with VLAN Transparency On. The Forwarding Rule selection parameter is also not applicable to transparent Service Profiles. All transparent Service Profiles share a single pre-configured Forwarding Rule, and a pre-configured QoS Profile for multicasts. The pre-configured Transparent Forwarding Rule can be modified but not deleted. For tagged packets, the VPL ID will be their VLAN tag. For untagged packets, the VPL ID will be None.
Priority Marking	The mode of marking data transmitted to the backbone network: Transparent, 802.1p or DSCP.
Priority Marking Value	Not applicable if the selected Priority Marking is Transparent. The marking value for data frames transmitted to the backbone, according to the configured Priority Marking: 0-63 for DSCP; 0-7 for 802.1p and 0 for Transparent.
Forwarding Rule	The Forwarding Rule used by the Service Profile. The Forwarding Rule parameter is not applicable (empty field) to transparent Service Profiles (VLAN Transparency On), as all transparent Service Profiles share the same pre-defined Forwarding Rule.
Deployment Count	The number of Base Stations/Micro Base Stations in which the Service Profile is defined. A count of 0 means that the Service Profile is defined only in the NMS database and is not used in any device. After modifying and re-deploying a Service Profile, the deployment count of the original profile is set to 0.

NOTE

If two (or more) Service Profiles with the same name but with different properties are defined in different Base Stations, they will be displayed as different entities (rows). Different properties may include: non matching value of any parameter of either the Service Profile or its components, or non matching name of a component.

To open the Service Profile Editor for creating a new Service Profile:

1. Click on the **New** button, or right-click on any table's entry to open the options selection box and select the **New** option. The Service Profile Type selection window opens.
2. Select the required Service Profile Type (L2, PPPoE or VoIP) from the drop-down menu and click on the **OK** button to open the Service Profile Editor.

To open the Service Profile Editor for editing an existing Service Profile:

Select the applicable table's entry and click on the **Open** button, or double-click on the selected entry, or right-click on the entry to open the options selection box and select the **Open** option.

To delete a Service Profile from the database:

Select the applicable table's entry and click on the **Delete** button, or right-click on the entry to open the options selection box and select the **Delete** option.

NOTE

A Service Profile can be deleted from the database only if it is not in use (deployed) in any Base Station (Deployment Count is 0).

4.3.2 The Service Profile Editor

The Service Profile Editor enables management of Service Profiles and their components, and deployment of Service Profiles in selected Base Stations.

The Service Profile Editor includes the following tabs:

- "General Tab
- "Forwarding Rule Tab
- "Priority Classifier Tab
- "Deployment Tab

4.3.2.1 Saving Templates

The Service Profile Editor enables saving Service Profile components (Forwarding Rules, Priority Classifiers and QoS Profiles) as Templates in the database, supporting reuse of these components.

To save a Service Profile component as a Template (after defining it), click on the **Save as Template** icon to open the Save Template dialog box. Enter the Template Name (must be unique in the database and up to 32 characters), and click on the **OK** button.

4.3.2.2 Reuse of Service Profile Components

The Service Profile Editor enables reuse of Service Profile components (Forwarding Rules, Priority Classifiers and QoS Profiles). This includes relevant components that are available either in the database (as Templates) or in the managed devices.

To use an existing component, click on the **Select** button to open the Select window for the relevant component.

4.3.2.2.1 Using and Managing Templates

To view all relevant entities in the database, click on the **Retrieve** button. To view only entities that meet certain selection criteria, click on the **Select Filters** button to narrow the search criteria, and then click on the **Retrieve** button to view the entities that match the selection criteria.

Select an entry and click on the **Select** button to use it in the Service Profile Editor.

You can also remove an entry from the database by selecting it and clicking on the **Delete** button. After confirmation it will be removed from the Templates database (it may still exist and be used in one or several devices).

A Service Profile component's Template cannot be edited: To modify a Template or its name, you must first delete it and then redefine it.

4.3.2.2.2 Using Components from Managed Devices

To view the relevant components that exist in the managed devices, click on the **Get from Device** button. To view all relevant entities in all managed devices, click on the **Retrieve** button. To view only entities that meet certain selection criteria, click on the **Select Filters** button to narrow down the search criteria, and then click on the **Retrieve** button to view the entities that match the selection criteria.

Select an entry and click on the **Select** button to use it in the Service Profile Editor.

4.3.2.3 General Tab

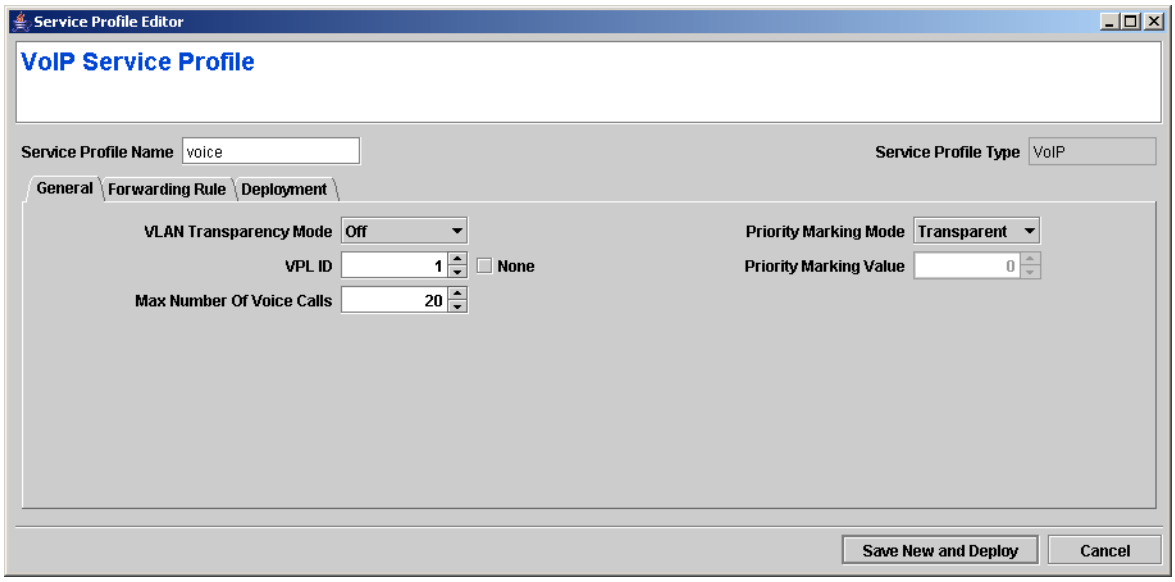

Figure 4-3: Service Profile Editor - General Tab

The General tab of the Service Profile Editor enables definition of the following Service Profile's parameters:

Parameter	Description
Service Profile Name	A Service Profile Name consists of up to 32 printable characters.
VLAN Transparency Mode	The VLAN Transparency Mode defines the method of transferring packets to the operator's upstream network. The options are On (Transparent Service Profile) or Off (Non-transparent Service Profile).
VPL ID	The VPL ID is the Virtual Private Link ID (or VLAN) to be used in the backbone behind the Base Station. The VPL ID parameter is not applicable to Service Profiles with VLAN Transparency Mode On (4096). Available values are in the range of 0 to 4094 or None (4095).
Max Number of Voice Calls	The upper limit on the number of simultaneous VoIP calls that can be supported by the Service using the Service Profile. This parameter is applicable only to L2 and VoIP Service Profiles, for calls made by devices that support the DRAP protocol. The available range is from 0 to 50 calls.
Priority Marking Mode	The mode of marking data transmitted to the backbone network: Transparent, 802.1p or DSCP. DSCP is (not applicable to PPPoE.

Parameter	Description
Priority Marking Value	Not applicable if the selected Priority Marking Mode is Transparent. The marking value for data frames transmitted to the backbone, according to the configured Priority Marking Mode. The range is: ■ Transparent: 0 ■ DSCP Marking Mode: 0 - 63 ■ 802.1p Marking Mode: 0 - 7

4.3.2.4 Forwarding Rule Tab

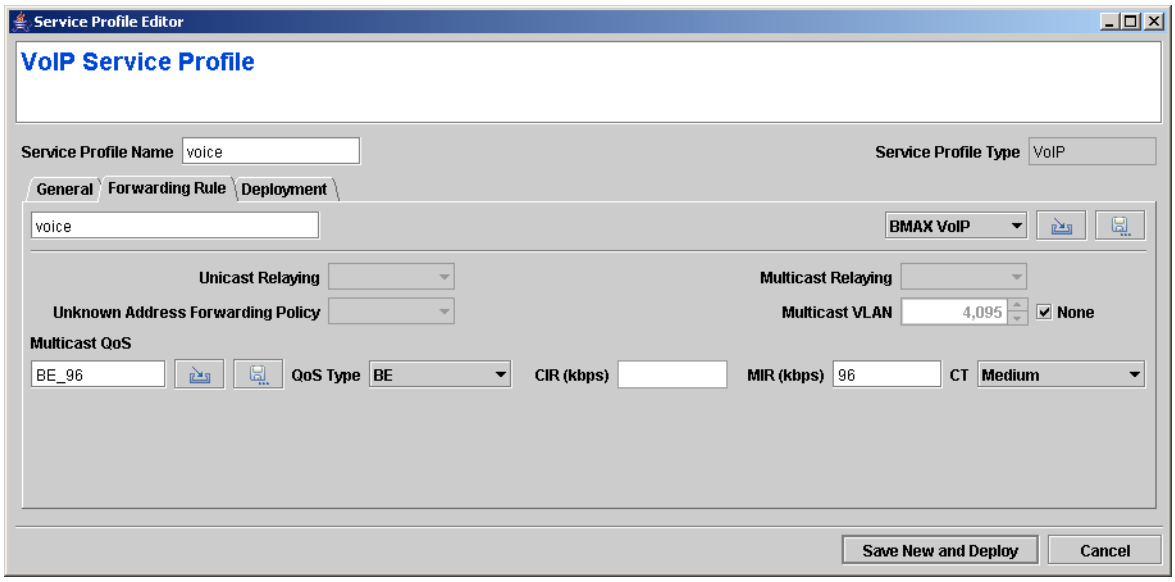

Figure 4-4: Service Profile Editor - Forwarding Rule Tab

The Forwarding Rule tab of the Service Profile Editor is not applicable to transparent Service Profiles (Transparent Service Profile On), in which a default Transparent Forwarding Rule is used. The Forwarding Rule tab enables definition of the following parameters:

Parameter	Description
Name	A Forwarding Rule Name consists of up to 32 printable characters. Enter a name for a new Forwarding Rule or use the **Select** button to use an existing Forwarding Rule.

Parameter	Description
Type	The Service Type: L2, PPPoE or VoIP. The Service Type of a Forwarding Rule in an L2 or VoIP Service Profile can be either L2 or VoIP (there is practically no difference). The Service Type of a Forwarding Rule in a PPPoE Service Profile is set to PPPoE.
Unicast Relaying	The Unicast Relaying parameter is applicable only to L2 and VoIP Services. The Unicast Relaying parameter determines whether the AU/Micro Base Station performs unicast relaying. When the Unicast Relaying parameter is enabled, unicast packets originating from devices on the wireless link can be transmitted back to the wireless link devices. If disabled, these packets are not sent to the wireless link even if they are intended for devices on the wireless link.
Multicast Relaying	The Multicast Relaying parameter is applicable only to L2 and VoIP Services. The Multicast Relaying parameter determines whether the AU/Micro Base Station performs multicast relaying. When the Multicast Relaying parameter is enabled, multicast packets originating from devices on the wireless link are transmitted by the AU/Micro Base Station back to the wireless link devices, as well as to the backbone. If disabled, these packets are sent only to the backbone and are not sent back to the wireless link.
Unknown Address Forwarding Policy	The Unknown Address Forwarding Policy parameter is applicable only to L2 and VoIP Services.The Unknown Address Forwarding Policy parameter determines the mode of controlling the flow of information from the backbone to the wireless media. Select from the following options: ■ Reject: The AU/Micro Base Station will transmit unicast packets only to those addresses that the AU/Micro Base Station knows to exist on the wireless link side. ■ Forward: Enables the transmission of all packets, except unicast packets sent to addresses that the AU/Micro Base Station recognizes as being on its wired backbone side.

Parameter	Description
Multicast VLAN	The Multicast VLAN ID parameter is applicable only to Services assigned to SUs with SW version below 2.0. The Multicast VLAN ID is the VLAN ID to be attached to mulicast messages in order to enable full support of the VLAN feature by SUs with SW version below 2.0. In SUs with SW version below 2.0, it was necessary to use behind the SU a VLAN switch with binding capability to support multiple VLAN IDs. The VLAN switch was responsible for duplicating all the packets to the correct ports according to the multicast connection, this required switch pre-configuration. If a VLAN switch with binding capability was not used, only a single VLAN ID behind the SU could be supported, and this VLAN ID has to be identical to the multicast VLAN ID. In the current version, all packets received from the wireless port over a multicast connection are transmitted by the SU several times to the Ethernet port, each time with a different VLAN ID, taken from the VLAN ID list supplied by the NPU/Micro Base Station. Available values are in the range of 0 to 4094 or None (4095) and 4096 for Transparent FwR.
Multicast QoS	The QoS Profile to be used in the downlink for multicasts. A QoS Profile Name consists of up to 32 printable characters. Enter a name for a new QoS Profile or use the Select button to use an existing QoS Profile.
QoS Type	The QoS Type: BE, NRT, RT or CG.
CIR (kbps)	Applicable only to RT and NRT QoS Types. The information transfer rate that the system is committed to transfer under normal conditions. The rate is averaged over a minimum increment of time, which is defined by the CT parameter. The range is from 0 to 12,000 Kbps. CIR cannot be higher than MIR (applicable to NRT QoS type).
MIR (kbps)	Applicable only to NRT and BE QoS Types. The maximum information rate that the system will allow for the connection. The rate is averaged over a minimum increment of time, which is defined by the CT parameter. The range is from 1 to 12,000 Kbps.

Parameter	Description
CT	Applicable for RT, NRT and BE QoS Types. The CT (Committed Time) parameter defines the time window over which the information rate is averaged to ensure compliance with the CIR or MIR parameter. It is used also to prioritize bandwidth allocation to connections, where for each QoS Type, connections with a shorter CT get higher priority. The available options are Short, Medium, and Long. The actual value in milliseconds for each of the three options varies according to the QoS type. For more details refer to the BreezeMAX System Manual.
PS (bytes)	Applicable only to CG QoS Type. The Packet Size parameter defines the amount of data in bytes that is expected for each grant. The range is from 64 to 1550 (bytes).
SI (ms)	Applicable only to CG QoS Type. The Sample Interval parameter defines the time in milliseconds between two successive grants (inter arrival time). The range is from 5 to 100 (milliseconds), using increments of 5 milliseconds.

4.3.2.5 Priority Classifier Tab

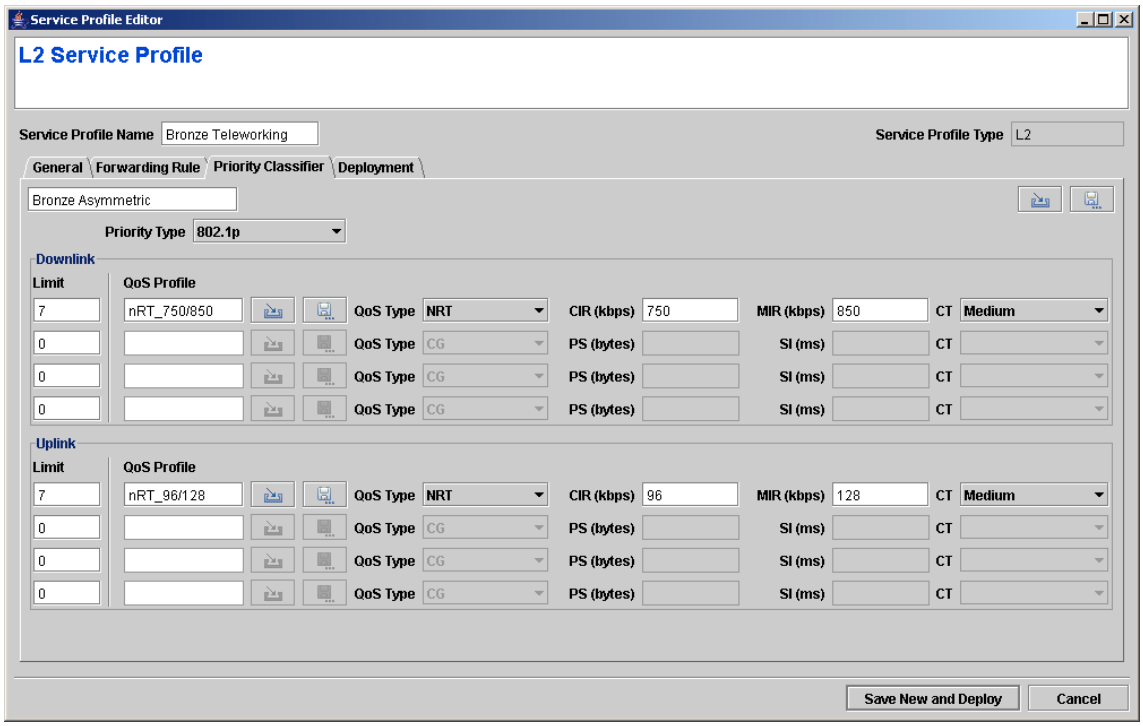

Figure 4-5: Service Profile Editor - Priority Classifier Tab

The Priority Classifier tab of the Service Profile Editor is not applicable to VoIP Service Profiles. The Priority Classifier tab enables definition of the following parameters:

Parameter	Description
Name	A Priority Classifier Name consists of up to 32 printable characters. Enter a name for a new Priority Classifier or use the **Select** button to use an existing QoS Profile.
Priority Type	The Priority Classifier Type: DSCP or 802.1p.

Parameter	Description
Uplink/Downlink Limits	The Uplink/Downlink Limit and QoS Profile parameters enable to define up to four ranges, where a different QoS Profile can be assigned to each range. The Limits (priority ranges) and assigned QoS Profiles are defined independently for the Uplink and Downlink, based on the upper Limit defined for each priority range. Up to 4 Limits (priority ranges), and the associated QoS Profiles, can be defined for each direction. A valid definition of Limits in each direction must comply with the following rules: ■ Each Limit must be higher than its predecessor. ■ The highest Limit must be the highest value available for the applicable priority type (7 for 802.1p, 63 for DSCP). ■ The same number of Limits (priority ranges) must be defined for the Uplink and Downlink. To define a Priority Classifier when no prioritization is used, select DSCP as the Priority Type, define 63 as the first Limit for both the Uplink and Downlink, and leave all other Limits empty. Alternatively, you can select 802.1p and define 7 as the Limit for both directions.
QoS Profile (for each defined (Uplink/Downlink Limit)	A QoS Profile must be associated with each defined Limit. A QoS Profile Name consists of up to 32 printable characters. Enter a name for a new QoS Profile or use the **Select** button to use an existing QoS Profile.
QoS Type (for each QoS Profile)	The QoS Type: BE, NRT, RT or CG.
CIR (kbps) (for each applicable QoS Profile)	Applicable only to RT and NRT QoS Types. The information transfer rate that the system is committed to transfer under normal conditions. The rate is averaged over a minimum increment of time, which is defined by the CT parameter. The range is from 0 to 12,000 Kbps. CIR cannot be higher than MIR (applicable to NRT QoS type).
MIR (kbps) (for each applicable QoS Profile)	Applicable only to NRT and BE QoS Types. The maximum information rate that the system will allow for the connection. The rate is averaged over a minimum increment of time, which is defined by the CT parameter. The range is from 1 to 12,000 Kbps.

Parameter	Description
CT (for each applicable QoS Profile)	Applicable for RT, NRT and BE QoS Types. The CT (Committed Time) parameter defines the time window over which the information rate is averaged to ensure compliance with the CIR or MIR parameter. It is used also to prioritize bandwidth allocation to connections, where for each QoS Type, connections with a shorter CT receive higher priority. The available options are Short, Medium, and Long. The actual value in milliseconds for each of the three options varies according to the QoS type. For more details refer to the *BreezeMAX System Manual*.
PS (bytes) (for each applicable QoS Profile)	Applicable only to CG QoS Type. The Packet Size parameter defines the amount of data in bytes that is expected for each grant. The range is from 64 to 1550 (bytes).
SI (ms) (for each applicable QoS Profile)	Applicable only to CG QoS Type. The Sample Interval parameter defines the time in milliseconds between two successive grants (inter arrival time). The range is from 5 to 100 (milliseconds), using increments of 5 milliseconds.

4.3.2.6 Deployment Tab

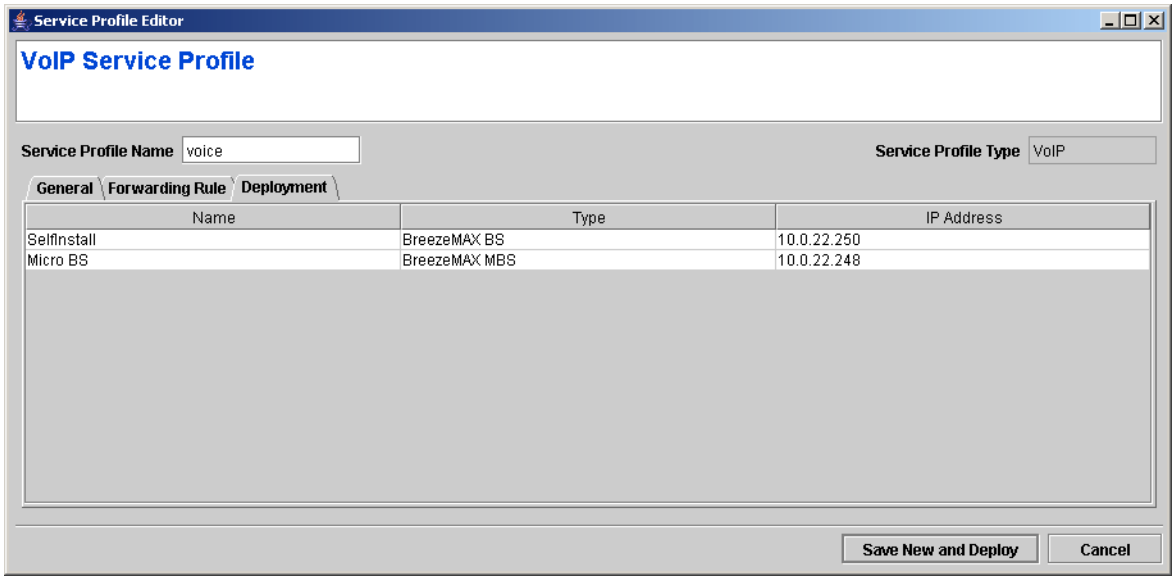

Figure 4-6: Service Profile Editor - Deployment Tab

The Deployment tab of the Service Profile Editor displays details on the Base Stations in which the Service Profile is currently deployed (empty for a new Service Profile). The details displayed for each Base Station include its Name, Type (BS or MBS) and IP Address.

4.3.2.7 Deploying Service Profiles

To deploy a new Service Profile, click on the **OK** button in any of the Service Profile Editor tabs to open the Service Profile Distribution Task.

To deploy an updated Service Profile, click on the **Save New and Deploy** button in any of the Service Profile Editor tabs to open the Service Profile Distribution Task. The deployment of an existing Service Profile without modifying any parameter can be done only from the task manager.

If there is any error in the defined Service Profile such as a missing parameter, contradicting definitions or non-valid value, the relevant error message(s) will be displayed at the top section of the window, and a red border around the relevant entries will indicate the parameters that should be corrected.

4.3.3 The Service Profile Distribution Task

The Service Profiles Distribution Task enables deployment of Service Profiles in one or more Base Stations. The Service Profile Distribution Task includes the following tabs:

- "General Tab
- "Equipment Tab
- "Service Profiles Tab

4.3.3.1 General Tab

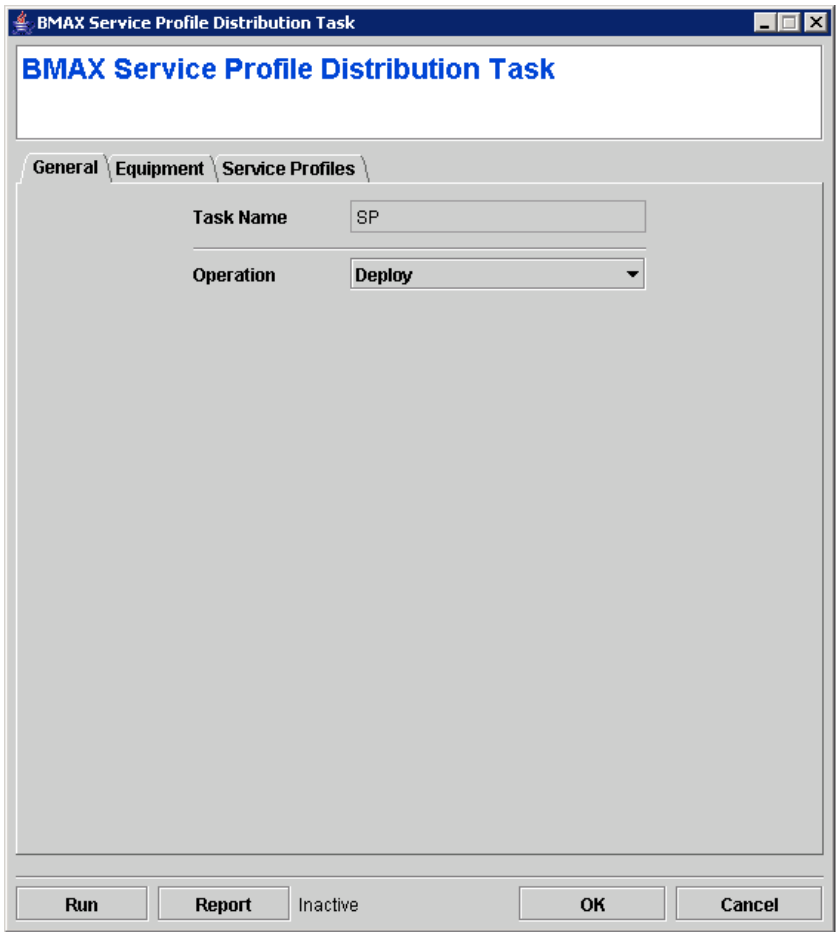

Figure 4-7: Service Profile Distribution Task - General Tab

The General tab of the Service Profile Distribution Task includes the following components:

Parameter	Description
Name	The name of the task. The default Name for a Service Profile Distribution Task is *<Service Profile Name>_<Date & Time>_Deployment*. It can be replaced with any other name. The Name must be unique (not allocated to any other task that exists in the database).

Parameter	Description
Operation	The requested operation: ■ Deploy: add the Service Profiles specified in the Service Profiles tab to the devices specified in the Equipment tab. ■ Undeploy: delete the Service Profiles specified in the Service Profiles tab from the devices specified in the Equipment tab.

4.3.3.2 Equipment Tab

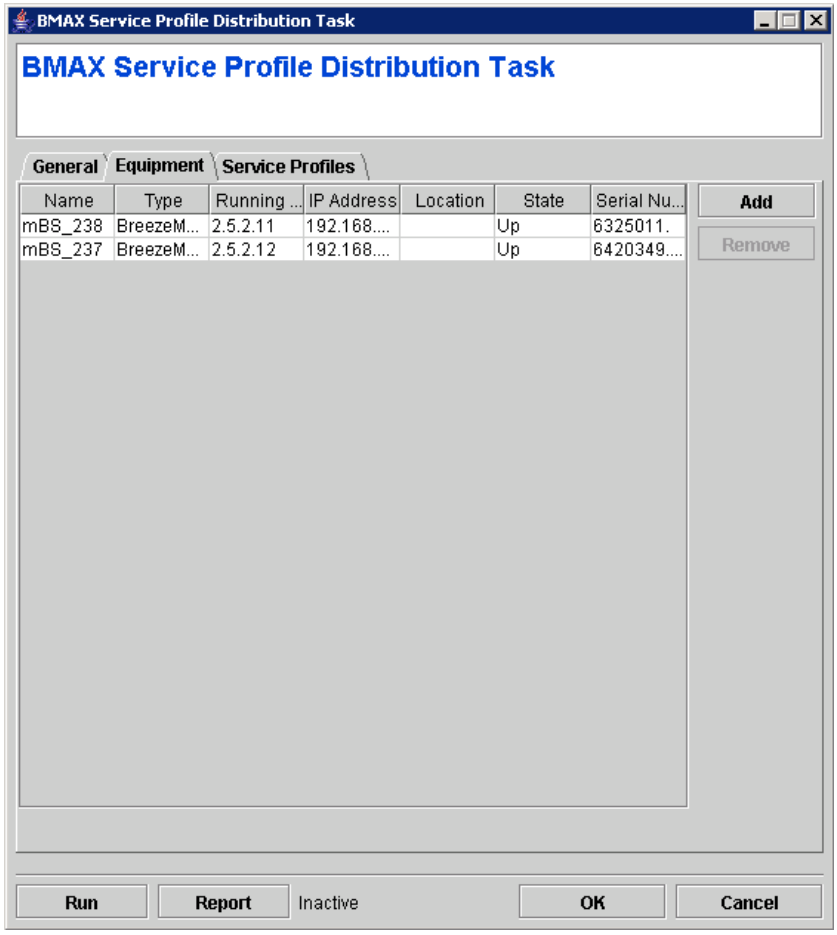

Figure 4-8: Service Profile Distribution Task - Equipment Tab

The Equipment tab enables managing the list of Base Station that will be included in the task.

Click on the **Add** button to open the Select Equipment window for selecting the devices to be added to the task.

Select one or several entries and click on the **Remove** button to remove the selected devices from the task.

4.3.3.3 Service Profiles Tab

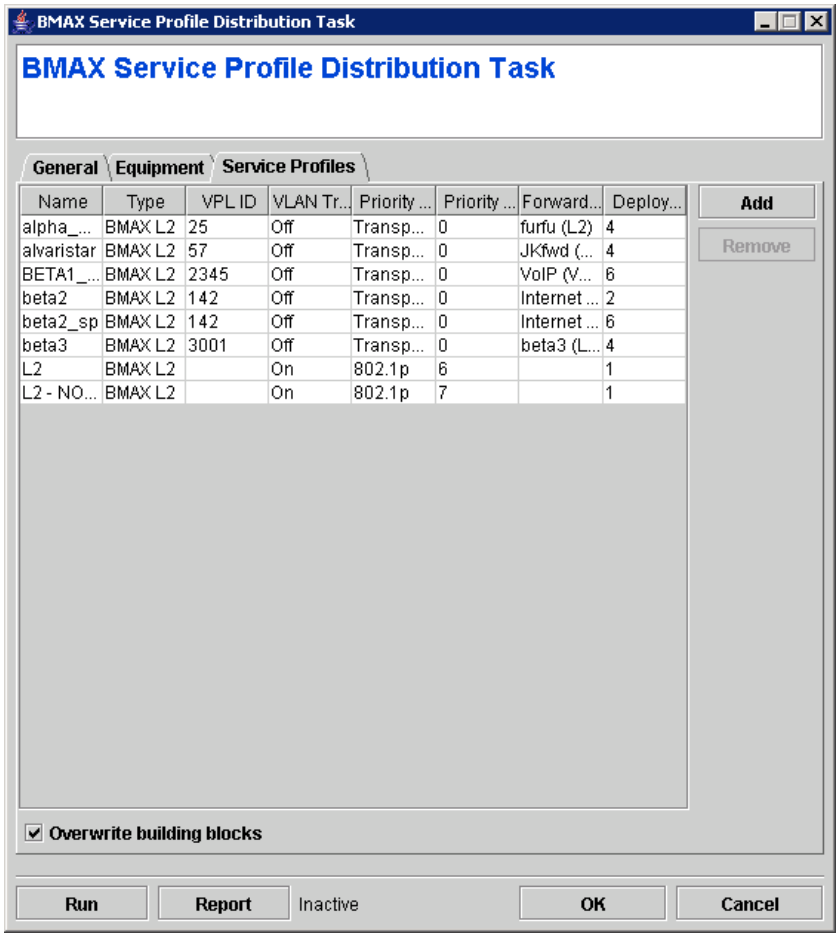

Figure 4-9: Service Profile Distribution Task - Service Profiles Tab

The Service Profiles tab enables managing the list of Service Profiles that will be included in the task.

Click on the **Add** button to open the Select Service Profiles window for selecting the Service Profiles to be added to the task.

Select one or several entries and click on the **Remove** button to remove the selected Service Profiles from the task.

When deploying Service Profiles, the target Base Stations may have Service Profile building blocks (Forwarding Rule, Priority Classifier, QoS Profiles) with the same names as the relevant components in the Service Profiles to be deployed, but with

different properties. Check the **Overwrite building blocks** checkbox to replace the relevant components in the target devices with the new component. Overwriting will, however, fail, if the type does not match. If you leave the checkbox unmarked (the default), a Service Profile will not be deployed (the operation will fail) if it includes one or more component with a matching name and different properties in the specific device.

4.4 Subscriber Manager

"The Subscriber Manager Window" - Section 4.4.1

"The Subscriber Editor" - Section 4.4.2

4.4.1 The Subscriber Manager Window

The Subscriber Manager window provides a comprehensive view of the current Subscribers defined in the entire network. This includes Subscribers that are defined in managed devices (deployed), and Subscribers that are defined only in the data base (undeployed). From the Subscriber Manager window you can:

- View currently defined Subscribers that exist in the database, according to various selection criteria
- Add or delete Subscribers to/from the database
- Open the Subscriber Editor for editing an existing Subscriber or creating a new one, and for deploying/undeploying/modifying Services allocated to a selected Subscriber.

To open the Subscriber Manager:

Select *Provisioning* > *Subscriber Manager* from the *File* > *Open* > *AlvariSTAR* menu or in the Navigation Pane.The Subscriber Manager window opens, with the default display of all Subscribers that exist in the database.

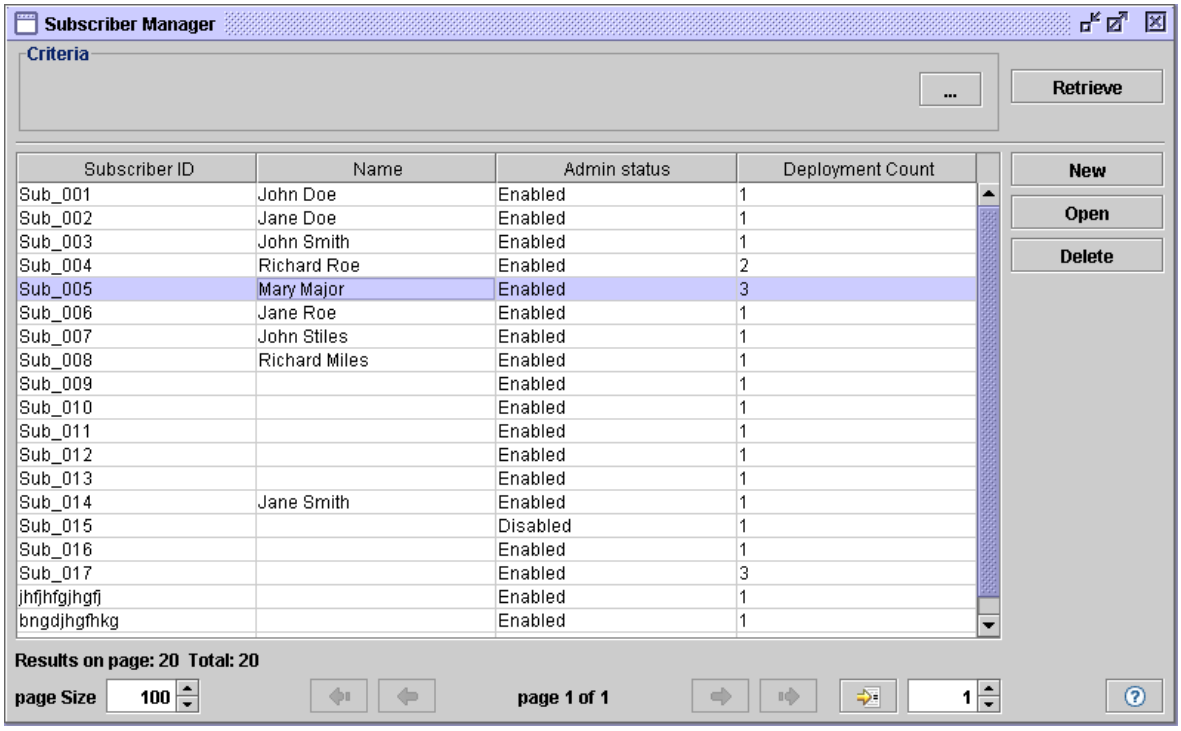

Figure 4-10: Subscriber Manager

To view Subscribers according to preferred selection criteria:

1 Click on the **Select Filters** button to narrow the search criteria. See Section 1.7.5.1.

2 Click on the **Retrieve** button to view the Subscribers that match the selection criteria.

The Subscribers table displays the following details for each of the applicable Subscribers:

Parameter	Description
ID	The Subscriber's unique ID
Name	The Subscriber's Name (First Name and Last Name).

Parameter	Description
Admin Status	The administrative status of the Subscriber, as configured in the Base Station(s). A situation where the Subscriber is defined in more than one Base Station (Deployment Count>1) and the Admin Status is not the same in all Base Stations, is indicated by a *Mixed* value for the Admin Status. For a Subscriber that is defined only in the database (Deployment Count=0), the default Admin Status is Unknown.
Deployment Count	The number of Base Stations/Micro Base Stations in which the Subscriber is defined (deployed). A count of 0 means that the Subscriber is defined only in the NMS database and is not used in any device.

NOTE

If two (or more) Subscribers with the same ID but with different properties (non matching First Name or Last Name) are defined in different Base Stations, they will be displayed as different entities (rows).

To open the Subscriber Editor for creating a new Subscriber:

1. Click on the **New** button, or right-click on any table's entry to open the options selection box and select the **New** option.
2. The Subscriber Type selection dialog box will open. Select the required **Subscriber Type** (in the current version the only option is BMAX Subscriber) from the drop-down menu and click on the **OK** button to open the Subscriber Editor.

To open the Subscriber Editor for editing an existing Subscriber:

Select the applicable table's entry and click on the **Open** button, or double-click on the selected entry, or right-click on the entry to open the options selection box and select the **Open** option.

To delete a Subscriber from the database:

Select the applicable table's entry and click on the **Delete** button, or right-click on the entry to open the options selection box and select the **Delete** option.

NOTE

A Subscriber can be deleted from the database only if it is not in use (defined) in any Base Station (Deployment Count is 0).

4.4.2 The Subscriber Editor

The Subscriber Editor enables management of Subscribers and deployment of Services in selected Base Stations.

The Subscriber Editor includes three tabs:

- "General Tab
- "Services Tab
- "Deployment Tab

4.4.2.1 General Tab

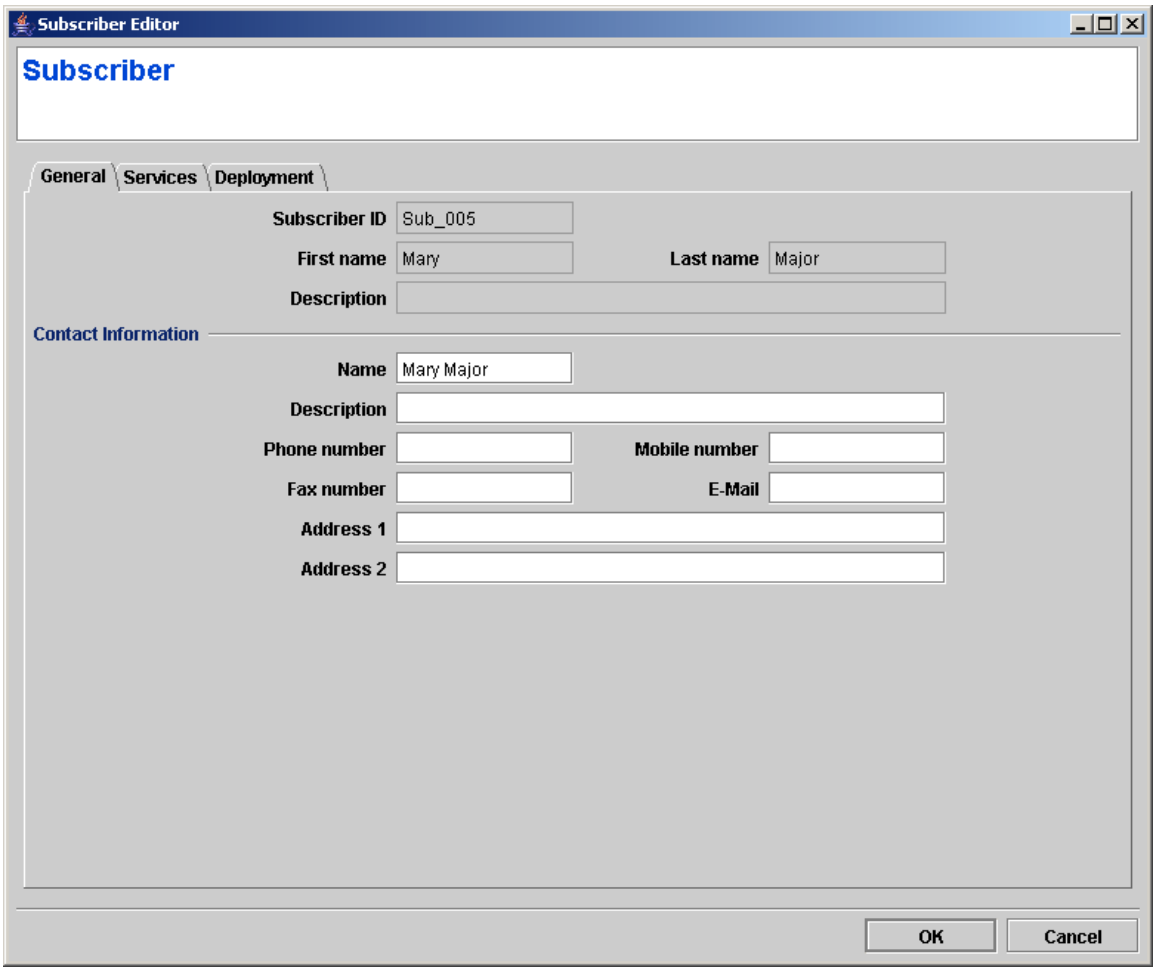

Figure 4-11: Subscriber Editor - General Tab

The General tab of the Subscriber Editor enables definition of the following Subscriber's parameters:

4.4.2.1.1 Subscriber General Details

These details are stored in the device(s) in which the Subscriber is defined. These details are definable only for a new Subscriber. For an existing Subscriber they cannot be changed, even if the Subscriber is not deployed in any Base Station.

Parameter	Description
Subscriber ID	A Subscriber ID (Name) consists of up to 32 printable characters The Subscriber ID must be unique for the entire network. The Subscriber ID of an existing Subscriber cannot be modified.

Parameter	Description
First Name	An optional parameter for information purposes. A First Name consists of up to 50 printable characters. The First Name of an existing Subscriber cannot be modified.
Last Name	An optional parameter for information purposes. A Last Name consists of up to 50 printable characters. The Last Name of an existing Subscriber cannot be modified.
Description	An optional parameter for information purposes. A Description consists of up to 50 printable characters. The Description of an existing Subscriber cannot be modified.

4.4.2.1.2 Subscriber Contact Information

These optional details are stored only in the NMS database for reference purposes:

Name, Description, Phone number, Mobile number, Fax number, E-mail address, 2 address fields.

4.4.2.2 Services Tab

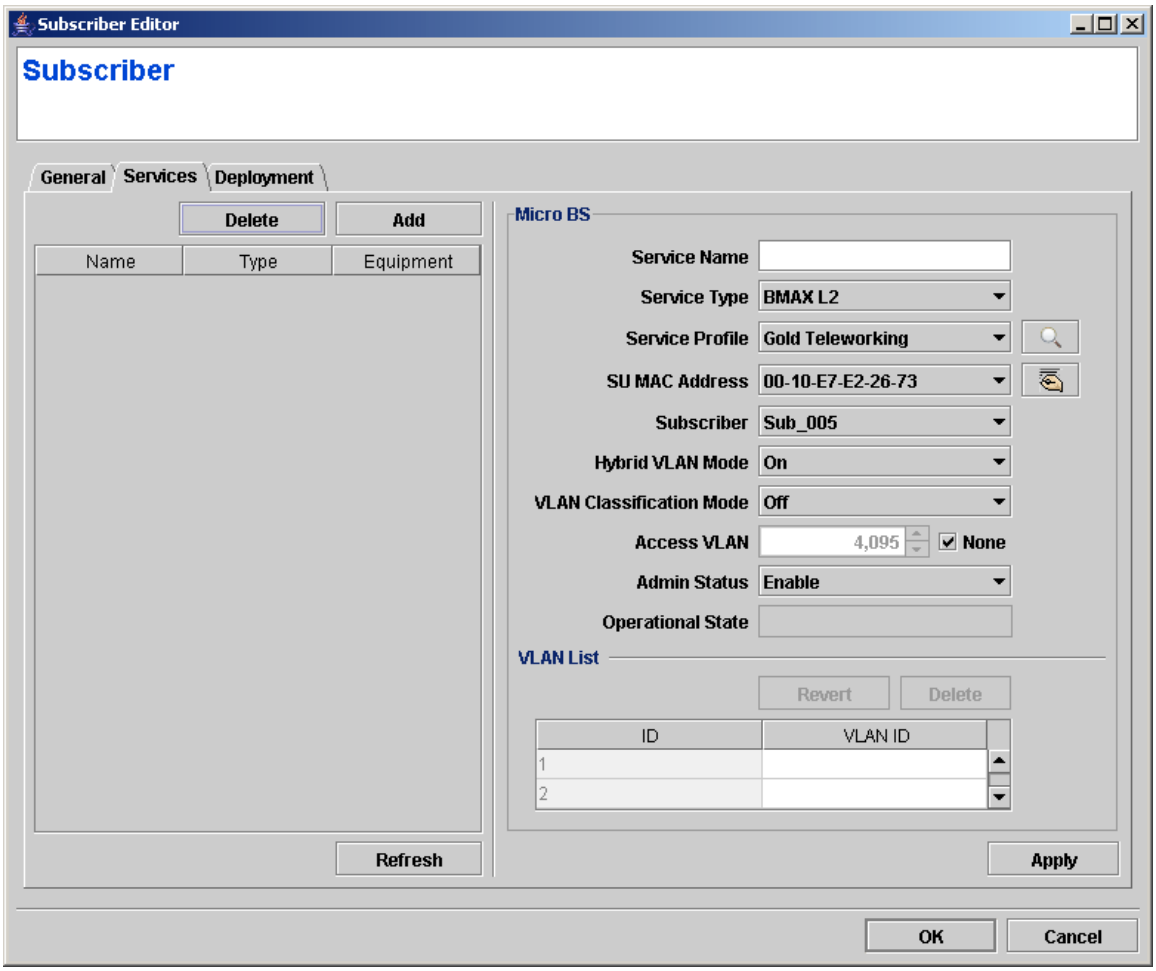

Figure 4-12: Subscriber Editor - Services Tab

The Services tab enables managing the list Services allocated to the Subscriber.

The Services table displays the general details of currently deployed Services allocated to the Subscriber. For each entry, the list includes:

Parameter	Description
Name	The Service Name
Type	The Service Type: L2, VoIP or PPPoE
Equipment	The Name and IP address of the Base Station in which the Service is deployed.

Select an entry to view and optionally modify a Service. The Service Editor will be displayed on the right side of the window.

To deploy the Subscriber in a new Base Station, and optionally add to it a Service, click on the **Add** button to open the Select Equipment window. After selecting the Base Station in which the new Service will be used, the Service Editor will be displayed, enabling to complete the definition of a new Service. If the subscriber does not exist in the Base Station, you will be asked to create it before a service can be created.

To delete a Service, select the relevant entry and click on the **Delete** button.

The Service Editor (on the right side of the window) includes the following components:

Parameter	Description
Name	The Services Name. A Service Name consists of up to 32 printable characters.
Service Type	The Service Type: L2, PPPoE or VoIP. The Service Type of an existing Service cannot be modified.
Service Profile	The Name of the Service Profile. The drop-down menu includes all Service Profiles with a matching Service Type that are available in the database of the Base Station/Micro Base Station. Click on the **Magnifying Glass** icon for a preview of the selected Service Profile properties.
SU MAC Address	The MAC Address of the SU associated with the Service. The SU MAC Address drop-down menu includes the MAC Addresses of all Permanent SUs in the database of the Base Station/Micro Base Station. Click on the **Hand** icon to add new MAC Addresses. The MAC Address of an existing Service can be modified only if the Admin Status of the Service is set to Disable (after applying the change).
Subscriber	The Subscriber ID as defined in the General tab.

Parameter	Description
Hybrid VLAN Mode	Hybrid VLAN Mode of operation enables classification of both tagged and untagged packets or untagged packets only, according to the following rules: ■ Hybrid VLAN Mode is Off and there is at least one VLAN in the VLAN List: Only packets tagged with a VLAN ID that exists in the VLAN List will be forwarded. The VLAN List can include up to 16 entries. ■ Hybrid VLAN Mode is Off and the VLAN List is empty: All (both untagged and tagged with any VLAN ID) will be forwarded. ■ Hybrid VLAN Mode is On and there is at least one VLAN in the VLAN List: Only untagged packets, and packets tagged with a VLAN ID that exists in the VLAN List, will be forwarded. The VLAN List can include up to 15 entries. ■ Hybrid VLAN Mode is On and the VLAN List is empty: Only untagged frames will be forwarded. Note that for each Service Type, a maximum of one Service that enables forwarding of untagged packets can be assigned to an SU. Forwarding of untagged packets is supported when either Hybrid VLAN Mode is On, or Hybrid VLAN Mode is Off and the VLAN List is empty. It is not possible to define for the same SU two Services of the same Service Type that enable forwarding of untagged packets. However, the same SU can be associated with two Services of different Service Types that enable forwarding of untagged packets, excluding the combination of L2 Service and VoIP Service.
VLAN Classification Mode	The VLAN Classification feature enables using VLAN ID (in addition to destination MAC address) for classification of transparent service downlink traffic before transmission to the destination MAC address. The VLAN Classification feature supports applications where multiple VLANs are associated with a single MAC address, allowing to assign different services to different VLANs. VLAN Classification Mode can be set to On only if the following conditions are met: ■ The VLAN Transparency Mode of the applicable Service Profile is set to On. ■ A single VLAN ID is defined for the Service. This means that the allowed combinations are: a) Hybrid VLAN Mode is Off and the VLAN List includes a single VLAN ID, or b) Hybrid VLAN Mode is On and the VLAN List is empty. ■ All Services assigned to the same SU must be configured with the same VLAN Classification Mode (Either On or Off).

Parameter	Description
Access VLAN	The Access VLAN parameter enables defining a VLAN ID to be used with untagged packets received on the Ethernet port of the SU. This parameter is applicable only for a transparent service (VLAN Transparency Mode is On) with Hybrid Mode set to On, or a transparent service with Hybrid Mode set to Off and an empty VLAN list. A tag with the defined Access VLAN will be added by the NPU/Micro Base Station to untagged packets in the uplink. The tag will be removed by the NPU/Micro Base Station from packets in the downlink. For a multicast connection, the NPU/Micro Base Station will send in addition to the VLAN list the single Access VLAN. The SU will be responsible for removing the Access VLAN if it is received on a multicast connection. The Access VLAN cannot be the same as the VPL ID in the applicable Service Profile(s). The range is from 0 to 4094 or None (4095).
Admin Status	The administrative status of the Service.
Operational State	A read-only display of the operational status. Up means that the Service is currently in use.
VLAN List	A table of VLAN IDs listing the VLAN IDs behind the same SU associated with the applicable Subscriber. When Hybrid VLAN Mode is Off, the VLAN List can include up to 16 VLAN IDs. When Hybrid VLAN Mode is On, the VLAN List can include up to 15 VLAN IDs (the 16th entry is reserved for No VLAN). To avoid conflicts it is not allowed to define a VLAN ID that is identical to any VPL ID (applicable only for transparent Service Profiles). A specific VLAN ID behind a certain SU can be associated only with a single service of a certain service type. It is not possible to define two services of the same service type for the same SU and the same VLAN ID. The maximum total number of VLAN IDs behind a single SU is 16. (15 when a Service with Hybrid VLAN Mode On is assigned to the SU). The VLAN ID’s value can be from 0 to 4094.

4.4.2.3 Deployment Tab

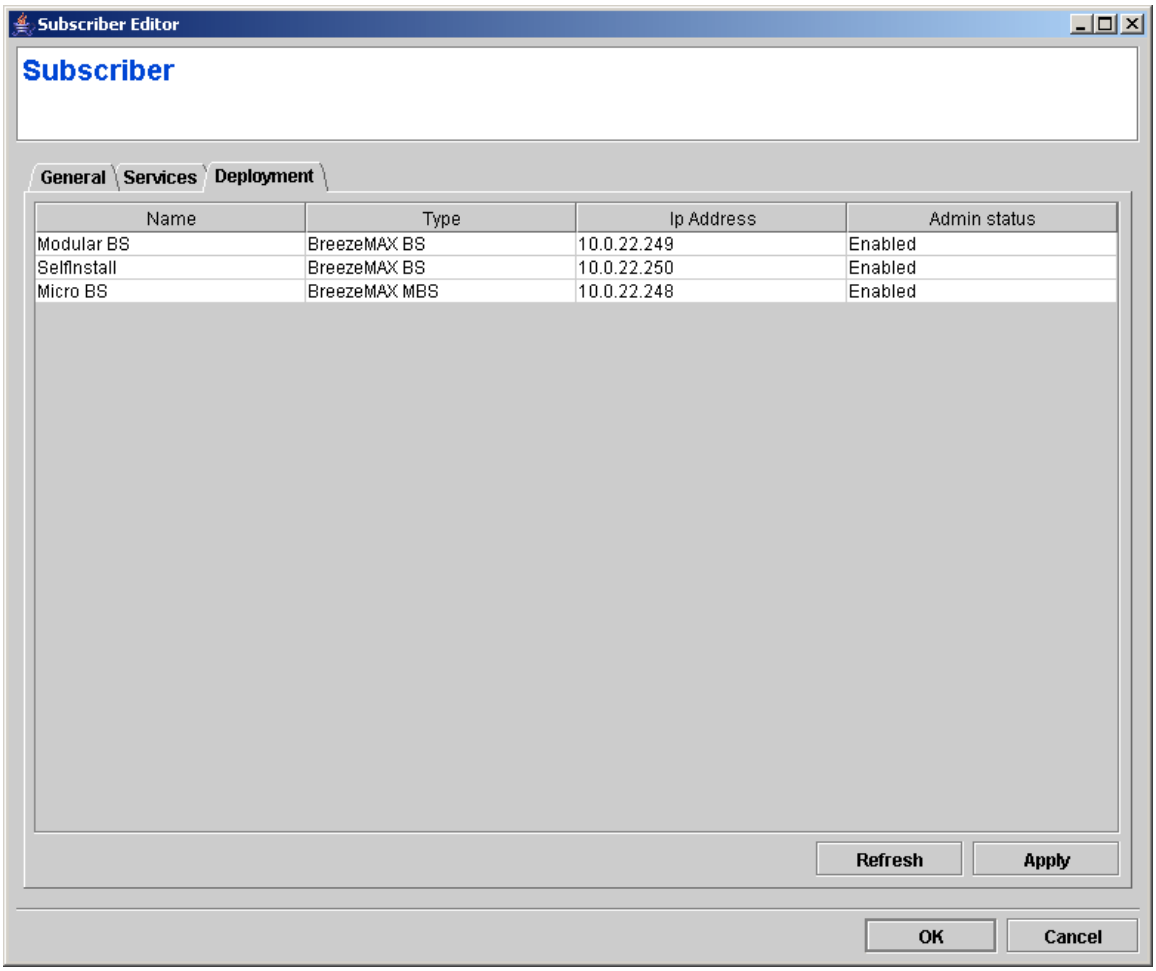

Figure 4-13: Subscriber Editor - Deployment Tab

The Deployment tab of the Subscriber Editor displays the general details of the Base Stations in which the Subscriber is defined (deployed), allowing to manage the Admin Status of the Subscriber in each Base Station.

For each Base Station in which the Subscriber is defined (deployed), the following parameters are displayed:

Parameter	Description
Name	The Name of the Base Station.
Type	The Type of Base Station: BS or MBS.
IP Address	The IP Address of the Base Station

Parameter	Description
Admin Status	The administrative status of the Subscriber in the Base Station: Enabled or Disabled. Double-click to change the Admin Status.

5

Chapter 5 - System Utilities

In This Chapter:

- “Introduction” on page 126
- “Task Manager” on page 127
- “License Manager” on page 157
- “User Monitor” on page 159
- “Audit Logs” on page 161

5.1 Introduction

The System Utilities node in the Navigation Pane comprises the following system-wide utilities:

- Task Manager - enables to manage system-wide tasks, such as SW upgrade, Network scan, PM collection, etc. See Section 5.2.
- License Manager - enables to view information about valid licenses. See Section 5.3.
- User Monitor - displays a list of currently logged in users. See Section 5.4.
- Audit Logs - enables to view information about actions performed in the system. See Section 5.5.

5.2 Task Manager

Tasks are operations that are performed on a large number of system entities (such as equipment, services, etc.). They run in the background, allowing the network administrators to continue managing the network while they run. After a task has completed, or upon termination of a task, a report is issued.

The Task Manager displays information on defined tasks and enables to create new tasks, edit, schedule, run or delete existing tasks. If there is any error in the parameters definition such as a missing parameter, contradicting definitions or non-valid value, the relevant error message(s) will be displayed at the top section of the window, and a red border around the relevant entries will indicate the parameters that should be corrected. The Task Manager also enables to abort running tasks and to view reports on completed and aborted tasks.

The following are the available types of tasks:

- "Network Scan Task" - Section 5.2.3
- "Database Aging Task" - Section 5.2.4
- "BreezeMAX Service Profile Distribution Task" - Section 5.2.5
- "Single Range Scan Task" - Section 5.2.6
- "Performance Collection Task" - Section 5.2.7
- "BreezeMAX Software Upgrade Task" - Section 5.2.8
- "BreezeMAX Configuration Backup Task" - Section 5.2.9

To open the Task Manager:

Select *System Utilities* > *Task Manager* from the *File* > *Open* > *AlvariSTAR* menu or the Navigation Pane. The Task Manager displays a list of defined tasks.

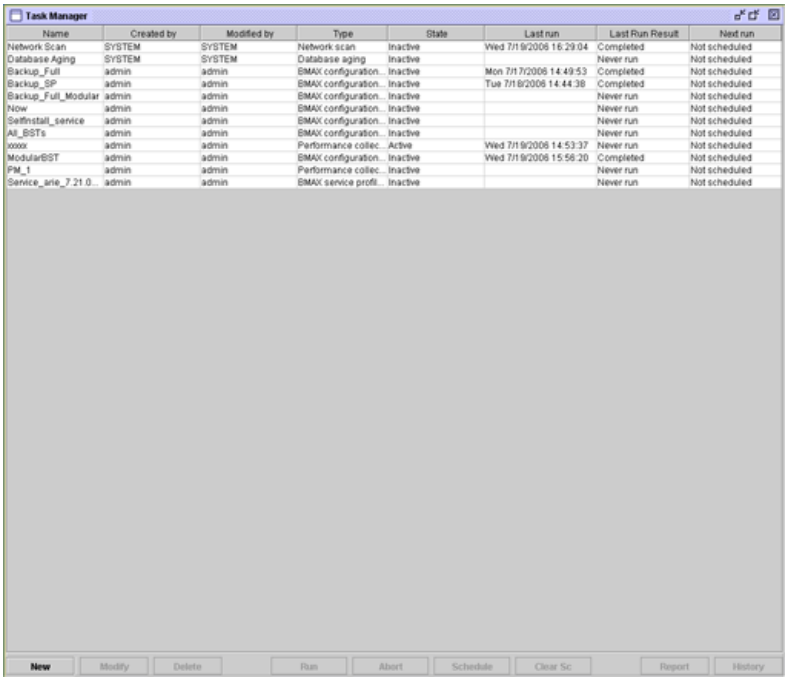

Figure 5-1: Task Manager

The following information is displayed for each defined task:

Parameter	Description
Name	The task's name. The name is unique in the system.
Created by	The user name of the task's creator.
Modified by	The name of the user who last modified the task.
Type	The type of task. The available task types are: ■ Network Scan Task ■ Database Aging Task ■ BreezeMAX Service Profile Distribution Task ■ Single Range Scan Task ■ Performance Collection Task ■ BreezeMAX Software Upgrade Task ■ BreezeMAX Configuration Backup Task
State	The current state of the task: Active/Inactive.

Parameter	Description
Last Run	The date and time the last time the task was run.
Last Run Result	The result of the task's last run: Completed/Completed with errors/Aborted/Never run.
Next Run	The date and time the next time the task is scheduled to run, or Not Scheduled.

The following are the controls of the Task Manager:

Parameter	Description
New	Adds a new task to the Task list. Click to select the type of task to be added, then click **OK**. The Task Editor for the selected task opens, allowing to set the task parameters. From the Task Editor, you can also run an inactive task by clicking **Run**.
Modify	■ For an Inactive Task: Opens the Task Editor for the selected Inactive task, allowing to edit the task parameters. Not available if more than one task is selected. From the Task Editor, you can also run the task by clicking **Run**. ■ For Active Task: Opens the Runtime Results window displaying the task's progress.
Delete	Deletes the selected task from the database. Select the task to remove and click **Delete**. The application prompts you for confirmation. Not available for active tasks and for system tasks (Network Scan Task and Database Aging Task). Scheduled tasks cannot be deleted. To delete a scheduled task, you need to first clear the schedule (see below).
Run	Manually executes the task. While the task is running, the state changes from Inactive to Active. The button is unavailable for currently running tasks. The Run button is also available in each of the task windows.
Abort	Aborts the selected running task. Available for running tasks only. Upon clicking on the **Abort** button, a confirmation message is displayed. Click **Yes** to abort the task. The task's *State* changes to *Inactive* and the *Last Run Result* to *Aborted*.
Schedule	Opens the Schedule Editor, enabling to schedule the activation of the task. See Section 5.2.1.
Clear Sc	Clears the schedule for the selected task. Active only for scheduled tasks.

Parameter	Description
Report	Opens the Task Report window, enabling to view a report of the last execution of the selected task. Not available for tasks that were never run. The Report window can also be accessed from each task editor. The Report button in the task editors is inactive while the task is running and will become active only after the task has completed. You can save the report to the file system by clicking the **Save As** button in the Task Report window. The system will prompt you to save large reports. Not available for tasks that were never run.
History	Opens the Task Results window, displaying a list of all past activations of the selected task and their results. Not available for tasks that were never run.

5.2.1 Scheduling Tasks

Tasks can be scheduled to run once, or at predefined recurrence intervals. Examples of non-recurring tasks include Software Upgrade and Service Profile Distribution; examples of recurring tasks include Network Scan and Database Aging.

To schedule a task:

1 In the Task Manager window, select a task from the list and click the **Schedule** button. The Schedule Editor opens.

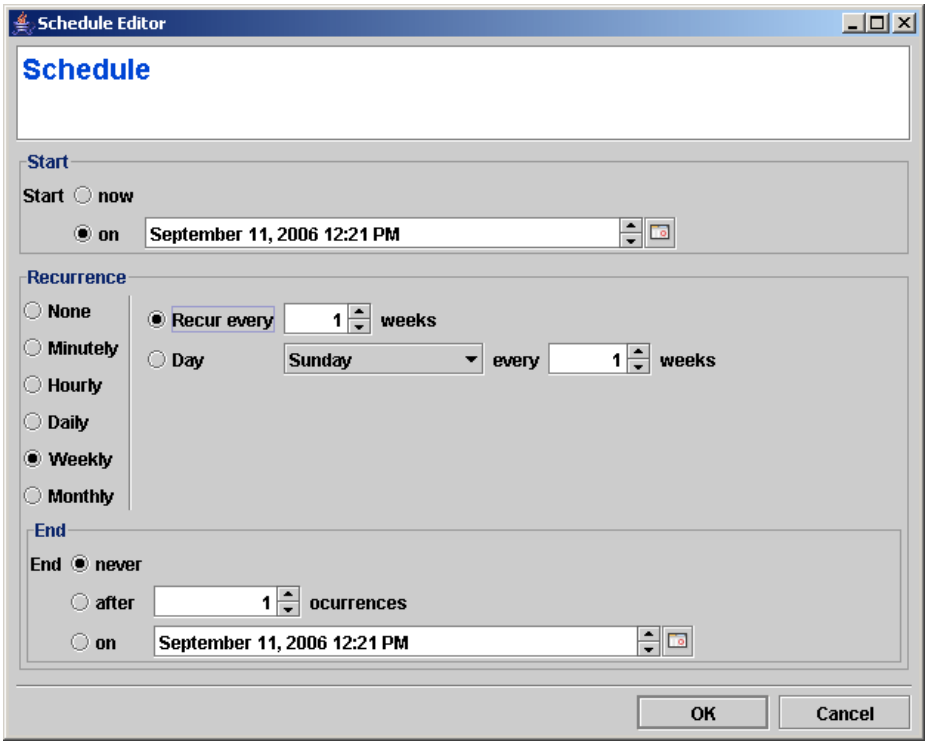

Figure 5-2: Schedule Editor

The Schedule Editor includes the following parameters:

Parameter	Description
Start	The start time for the task. Select one fo the following options: ■ Now ■ On - set a specific start date and time. You can highlight the value to change (month, day, year) and click on the up/down arrows to change the value, or you can pick a specific date using the calendar icon. You can also type in the date and time as follows: MMMM DD, YYYY HH:MM AM/PM.

Parameter	Description
Recurrence	Set the recurrence interval between each task execution. Available intervals include: ■ None - no recurrence (default) ■ Minutely - specify the number of minutes. (the range is 1-1,440) ■ Hourly - specify the number of hours. (the range is 1-96). ■ Daily - specify the number of days. (the range is 1-60) ■ Weekly - select one of the following options: ◇ Recur every - enter the number of weeks between task executions (the range is 1-20) ◇ Day - specify the day of the week (Sunday to Saturday) and the number of weeks between task executions (the range is 1-20). ■ Monthly - select one of the following options: ◇ Recur every - enter the number of months between task executions (the range is 1-36) ◇ Day - specify the day in the month (1-31) and the number of months between task executions (the range is 1-36).
End	The end time for a recurring task (only). Select one of the following options: ■ Never - enable tasks to be executed indefinitely ■ After N occurrences (where N is a number between 1-65,000) - set the number of occurrences after which the task's scheduling will be cleared. ■ On - set an end date and time. You can highlight the value to change (month, day, year) and click on the up/down arrows to change the value, or you can pick a specific date using the calendar icon. You can also type in the date and time as follows: MMMM DD, YYYY HH:MM AM/PM.

2 Set the **Start** and **End** time and optionally select a recurrence interval.

3 Click **OK** to apply the schedule for the selected task.

5.2.2 The Task Results Viewer

The Task Results window displays a list of all past activations of the task selected in the Task Manager window and their results. Not available for tasks that were never run.

To open the Task Results window:

In the Task Manager window, select a task from the list and click the **History** button. The Task Results window is displayed.

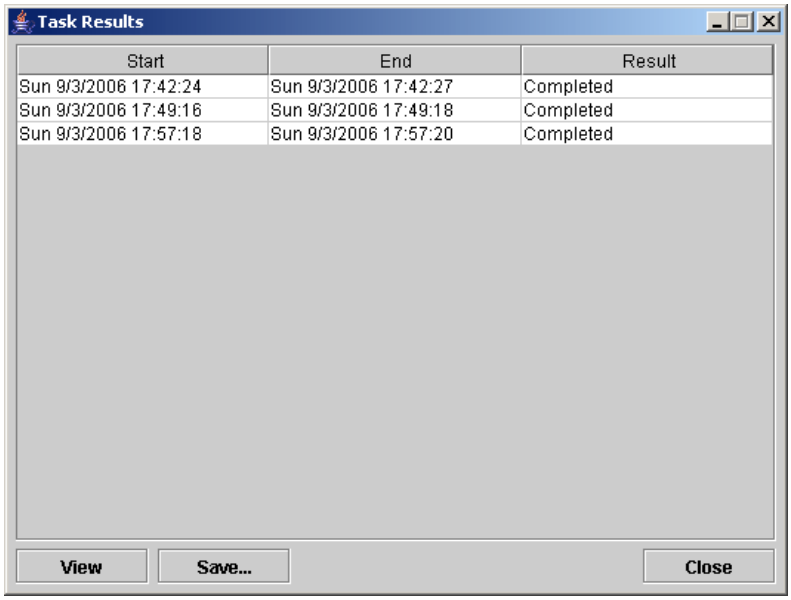

Figure 5-3: Task Results Window

The task Results window displays the following information for each listed activation:

Parameter	Description
Start	The start time of the activation.
End	The end time of the activation.
Result	The result of the activation.

The Task Results window includes the following controls:

Parameter	Description
View	Opens the Task Report viewer for the selected row. See Section 5.2.
Save	Enables to save the task results to an external file. Click and browse to a location in the file system, enter a name for the file and click **Save**.
Close	Closes the Task Results window.

5.2.3 Network Scan Task

The Network Scan task is a system task that scans the entire network for new devices. The scope of the network is defined in the Managed Network window (see Section 3.1). The Network Scan task can only be modified, not deleted.

To edit the Network Scan Task

1 In the Task Manager window, select the Network Scan task from the list and click **Modify**. If the task is Active, the Runtime Results window is displayed, displaying the status of the running task.

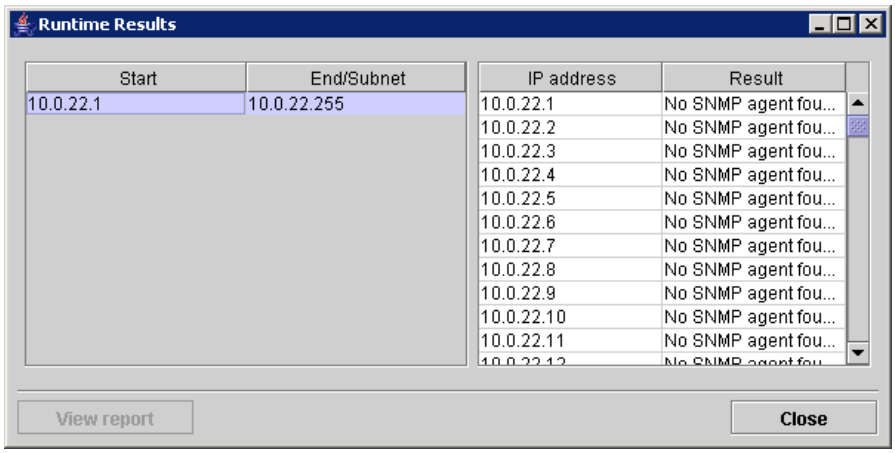

Figure 5-4: Network Scan Task - Runtime Results

If the task is Inactive, the Network Scan Task is displayed.

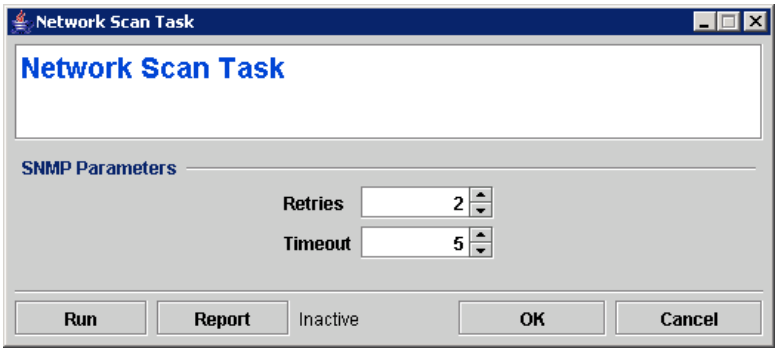

Figure 5-5: Network Scan Task Window

The Network Scan Task window includes the following parameters:

Parameter	Description
SNMP Parameters	
Retries	The maximum number of retries for SNMP/TFTP communication. The range is from 0 to 255.
Timeout	The maximum time in seconds that the requesting process waits for a response before attempting a retransmission (or aborting if the maximum number of retries has been reached). The available range is 1 to 3,600 seconds.

2 Change the parameters as required and click **OK** to save the changes and close the task window, **Cancel** to close the window without saving, or **Run** to execute the task. The adjacent field display changes from Inactive to Active, until the task has completed. When completed, you can view the report from the Task Editor or from the Task Manager.

5.2.4 Database Aging Task

The Database Aging task automates your database management tasks for records of alarm and audit logs that may otherwise overwhelm it. The Database Aging task is a system task and can only be modified, not deleted.

To edit the Database Aging Task:

1 In the Task Manager window, select the Database Aging task from the list and click **Modify**. If the task is Active, the Runtime Results window is displayed, displaying the status of the running task.

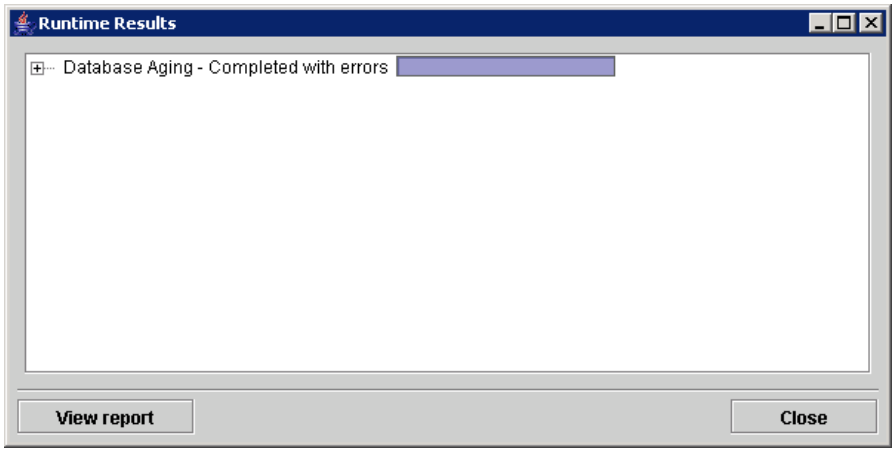

Figure 5-6: Database Aging Task - Runtime Results

If the task is Inactive, the Database Aging Task is displayed.

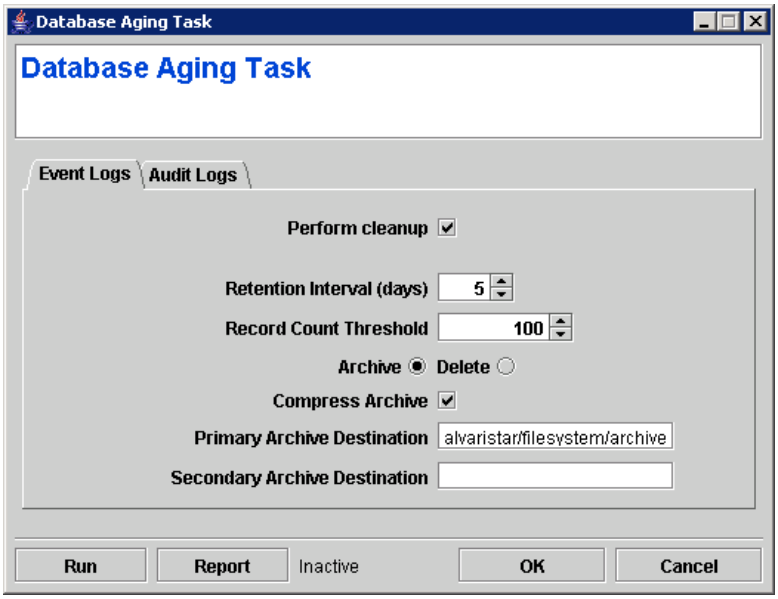

Figure 5-7: Database Aging Task Window

The Database Aging Task window includes two tabs:

- Event Logs - enables to automate the management of events
- Audit Logs - enables to automate the management of audit logs

Each tab comprises the following fields:

Parameter	Description
Perform cleanup	Check to enable cleanup of event/audit logs.
Retention Interval (days)	Determines how long to retain records (in days). The range is: 0 to 365 The default is: 90
Record Count Threshold	The number of records that will remain after the task completes. The range is: 0 to 2.000.000.000. The default is: 1.000.000
Archive/Delete	Determines whether to archive or permanently delete records, when the Retention Interval deadline is reached. The default is: Archive
Compress Archive	Checkbox that enables compression of the archive. Available only if *Archive* was selected (not *Delete*). The default is: Enabled (checked)
Primary Archive Destination	A disk location for archiving. The default location is: AlvariSTAR/filesystem/archive
Secondary Archive Destination	A disk location for archiving if the primary location fails.

2 Change the parameters as required and click **OK** to save the changes and close the task window, **Cancel** to close the window without saving, or **Run** to execute the task. The adjacent field display changes from Inactive to Active, until the task has completed. When completed, you can view the report from the Task Editor or from the Task Manager.

5.2.5 BreezeMAX Service Profile Distribution Task

The Service Profiles Distribution Task enables deployment of Service Profiles in one or more Base Stations.

To open the Service Profile Distribution Task window:

1 In the Task Manager window:

- Click **New**, select Service Profile Distribution from the list of available task types and click **OK**, the Service Profile Distribution window is displayed.

OR

- Select an existing Service Profile Distribution task from the list and click **Modify**. If the task is Active, the Runtime Result window is displayed, displaying the status of the running task.

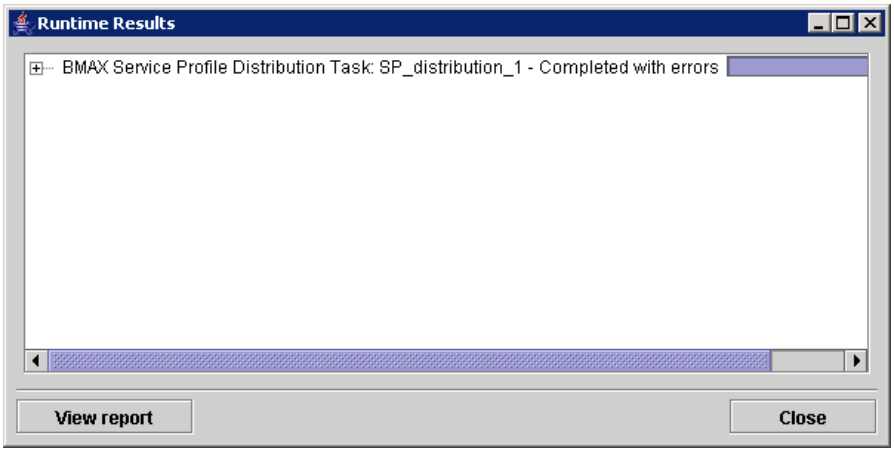

Figure 5-8: Service Profile Distribution Task - Runtime Results

If the task is Inactive, the Service Profile Distribution Task is displayed. See Section 4.3.3 for a detailed description of the Task.

5.2.6 Single Range Scan Task

The Single Range Scan Task enables to scan a predefined range of IPs for new and modified devices.

To open the Single Range Scan Task window:

1 In the Task Manager window:

- Click **New**, select Single Range Scan from the list of available task types and click **OK**, the Single Range Scan Task window is displayed.

OR

- Select an existing Single Range Scan task from the list and click **Modify**. If the task is Active, the Runtime Result window is displayed, displaying the status of the running task.

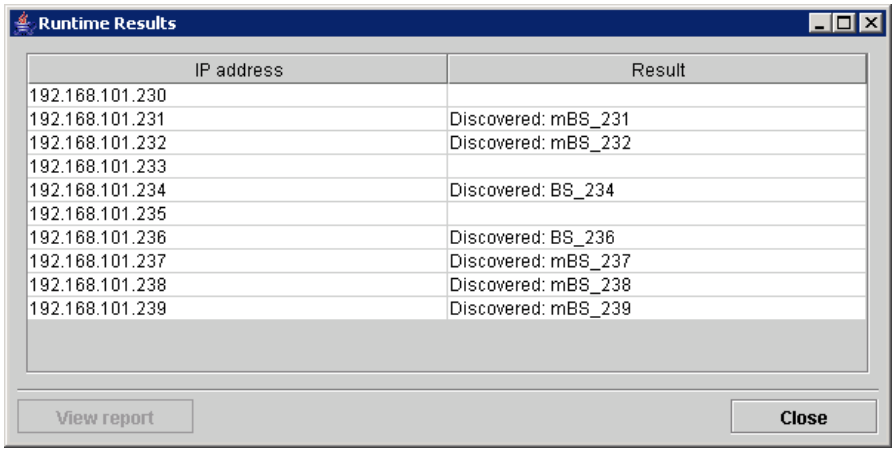

Figure 5-9: Single Range Scan Task - Runtime Results

If the task is Inactive, the Single Range Scan Task window is displayed.

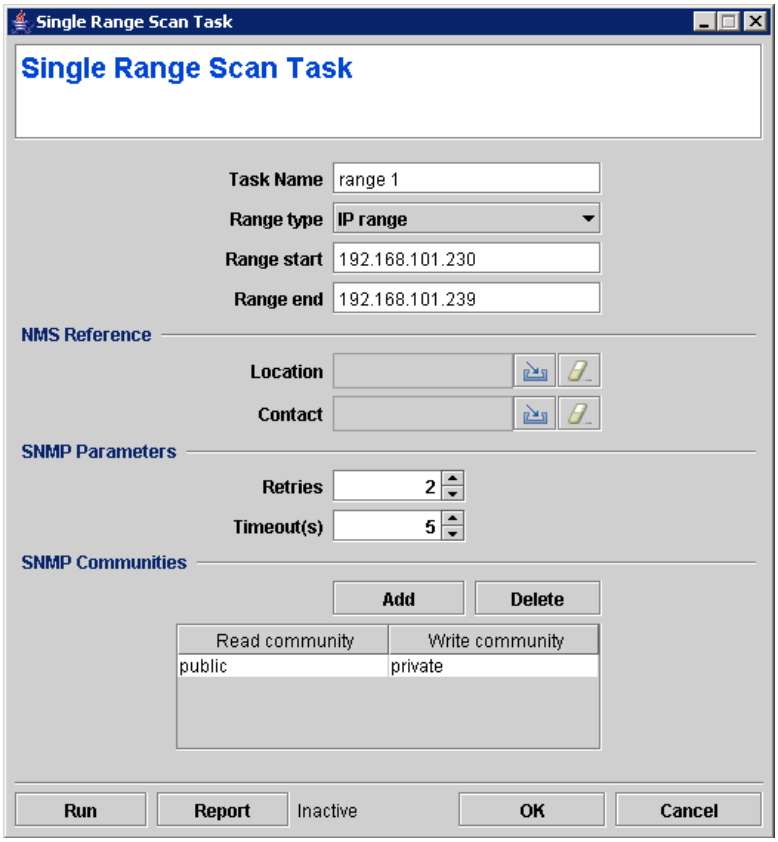

Figure 5-10: Single Range Scan Task Window

The Single Range Scan Task window comprises the following fields:

Parameter	Description
Task Name	The name of the task. A string of up to 255 printable characters. The name must be unique in the system.
Range Type	The range type: IP or Subnet.
Range Start	The first IP/Subnet in the range, depending on the selected Range Type.
Range End	The last IP/Subnet in the range, depending on the selected Range Type.
NMS Reference	
Location	An optional field for defining a location for devices in the range. Select from the available locations. Newly discovered devices will be automatically associated with the defined location. Devices already in the database will not be affected.
Contact	An optional field for defining a contact for devices in the range. Select from the available contacts. Newly discovered devices will be automatically associated with the defined contact. Devices already in the database will not be affected.
SNMP Parameters	
Retries	The maximum number of retries for SNMP/TFTP communication. The range is from 0 to 255.
Timeout(s)	The maximum time in seconds that the requesting process waits for a response before attempting a retransmission (or aborting if the maximum number of retries has been reached). The available range is 1 to 3,600 seconds.
SNMP Communities	
Read/Write Community	The community strings (passwords) for SNMP operations. These strings are used by the SNMP agent to allow/disallow SNMP access.

2 Edit the parameters as required and click **OK** to save the changes and close the task window, **Cancel** to close the window without saving, or **Run** to execute the task. The adjacent field display changes from Inactive to Active, until the task has completed. When completed, you can view the report from the Task Editor or from the Task Manager.

5.2.7 Performance Collection Task

The Performance Collection TaskPerformance Collection Task enables to collect performance data at defined intervals from specific equipment. It also enables to select the type of data to be collected.

To open the Performance Collection Task window:

1 In the Task Manager window:

- Click **New**, select **Performance Collection** from the list of available task types and click **OK**. The Performance Collection Task window is displayed.

OR

- Select an existing Performance Collection task from the list and click **Modify**. If the task is Active, the Runtime result screen is displayed, displaying the status of the running task.

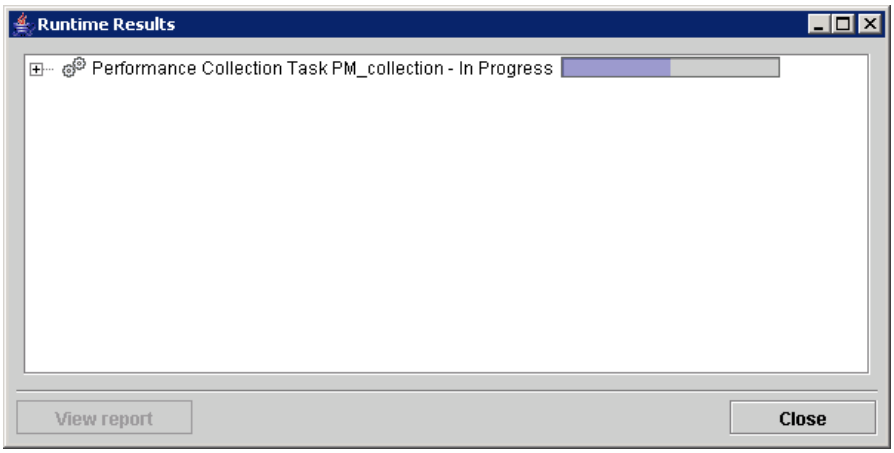

Figure 5-11: Performance Collection Task - Runtime Results

If the task is Inactive, the Performance Collection Task window is displayed.

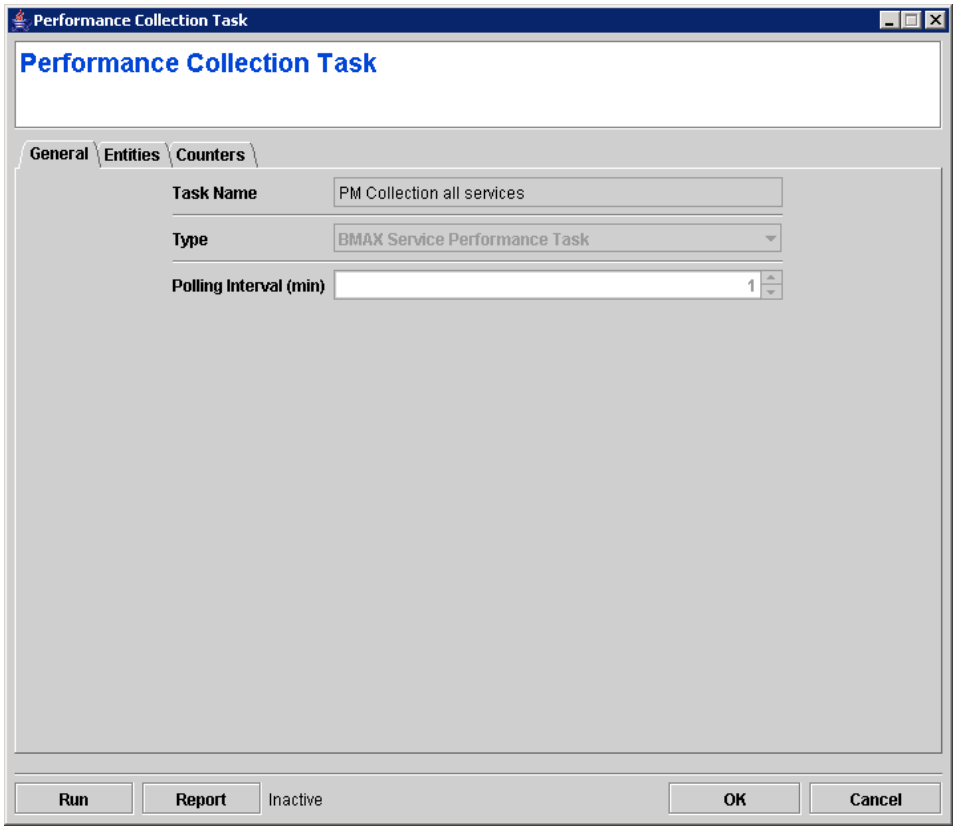

Figure 5-12: Performance Collection Task Window

The Performance Collection Task window includes three tabs:

- ◇ "General Tab" - Section 5.2.7.1
- ◇ "Entities Tab" - Section 5.2.7.2
- ◇ "Counters Tab" - Section 5.2.7.3

2 Change the parameters as required and click **OK** to save the changes and close the task window, **Cancel** to close the window without saving, or **Run** to execute the task. The adjacent field display changes from Inactive to Active, until the task has completed. When completed, you can view the report from the Task Editor or from the Task Manager.

5.2.7.1 General Tab

The General tab of the Performance Collection task enables definition of the following parameters:

Parameter	Description
Task Name	The name of the task. The name must be unique. This field is read-only when modifying an existing task.
Type	The type of data to be collected: *Service Performance task* or *Equipment Performance* task. This field is read-only when modifying an existing task.
Polling Interval (min)	The time (in minutes) between polls. The range is 1-60. This field is read-only when modifying an existing task.

5.2.7.2 Entities Tab

The Entities tab enables to select existing entities for performance collection. The type of entities depend on the selected Type in the General tab (equipment/services).

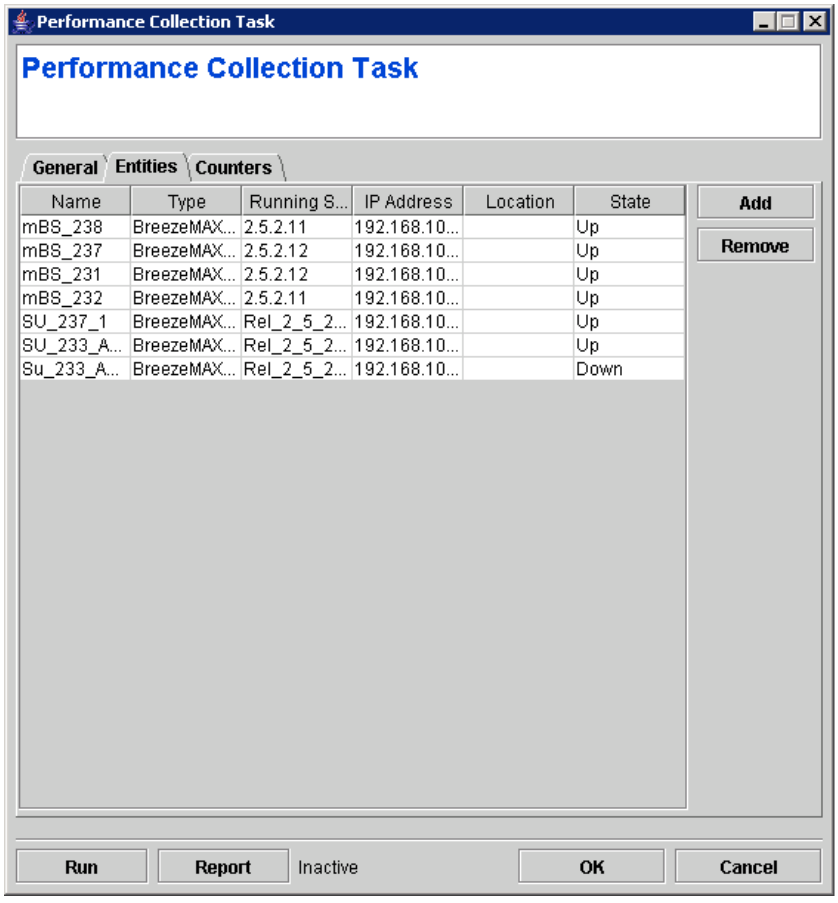

Figure 5-13: Performance Collection Task - Entities Tab (for Equipment)

The Entities tab includes the following controls:

Parameter	Description
Add	■ For Equipment Performance Task Type - opens a submenu with the following options: ◇ Base Stations - opens the Equipment selection window with the list of available Base Stations ◇ SUs - opens the Equipment selection window with a list of available SUs. ■ For Services Performance Task Type - opens the Service Selection window.
Remove	Removes selected entities from the list.

The following information is displayed for each added entity in the list:

■ For Equipment:

Parameter	Description
Name	The name of the Base Station/SU.
Type	The type of device: BreezeMAX BS, BreezeMAX MBS, BreezeMAX SU.
Software Version	The software version loaded on the device.
IP Address	The IP address of the Base Station.
Location	The location associated with the equipment.
State	The operational state of the equipment: Up/Down/Unreachable/ Unlicensed/Unknown

■ For Services:

Parameter	Description
Name	The Service Name
Type	The Service Type: L2, PPPoE or VoIP.
Admin Status	The administrative status of the Service.
Oper Status	The operational status of the Service. Up means that the Service is currently in use.
Service Profile	The Name of the Service Profile used in the Service.
Subscriber	The ID (Name) of the Subscriber to which the Service is allocated.
SU MAC Address	The MAC Address of the SU associated with the Service.

Parameter	Description
BS	The Name of the Base Station/Micro Base Station providing the Service.

5.2.7.3 Counters Tab

The counters tab enables to select the counters for the performance collection task. The list of counters depends on the type of performance task selected (equipment/services).

Figure 5-14: Performance Collection Task - Counters Tab

To select counters:

1 Click on the required counter in the Categories side to select it. More than one counter can be selected.

2 Click on the **Add** button, or double-click on the selected counter. The counter is displayed in the list of selected counters on the right.

The following are the available counters for selection:

- For Equipment performance:
  - SU Ethernet Rx
  - SU Ethernet Tx
  - Management Port Rx
  - Data Port Rx
  - Management Port Tx
  - Data Port Tx
  - Wireless Rx
  - Wireless Tx
  - AU Back-Panel
  - Radio
- For Services performance:
  - Uplink RT-VR, NRT-VR, BE Services Statistics
  - Downlink RT-VR, NRT-VR, BE Services Statistics

For the exact nature of each counter, refer to the *Device Manager User Manual*.

5.2.8 BreezeMAX Software Upgrade Task

Software upgrade is performed by loading the requested software files to the shadow memory of the devices using TFTP, and activating the new software version at a desired moment according to a predetermined process.

It is possible to define any number of software upgrade tasks that will be executed independently of each other. Up to 20 concurrent TFTP uploading sessions can run on the Application Server.

Software upgrade consists of several actions that need to be performed:

- Selecting devices to be included in each software upgrade task

- Defining the software file(s) to be loaded
- Scheduling the task (optional)
- Defining the actions that should take place once the new software file is loaded into the devices.

When working under Windows, the files to be loaded should be available in the Application Server firmware folder located by default under

<Drive ID>\AlvariSTAR\filesystem\firmware\rb, where *Drive ID* is the applicable location of the AlvariSTAR installation. The *rb* folder may need to be manually created.

When working under UNIX, refer to the instructions in:

/opt/AlvariSTAR/firmware/rb

The system will automatically identify the files and use the correct file for each device type. To ensure a smooth upgrade process while minimizing the risk of loosing connectivity to devices, the order of upgrading devices depends on device types (first the SUs, then AUs, etc.).

To open the Software Upgrade Task window:

1 In the Task Manager window:

◇ Click **New**, select **Software Upgrade** from the list of available task types and click **OK**. The Software Upgrade Task window is displayed.

OR

◇ Select an existing Software Upgrade task from the list and click **Modify**. If the task is Active, the Runtime result screen is displayed, displaying the status of the running task.

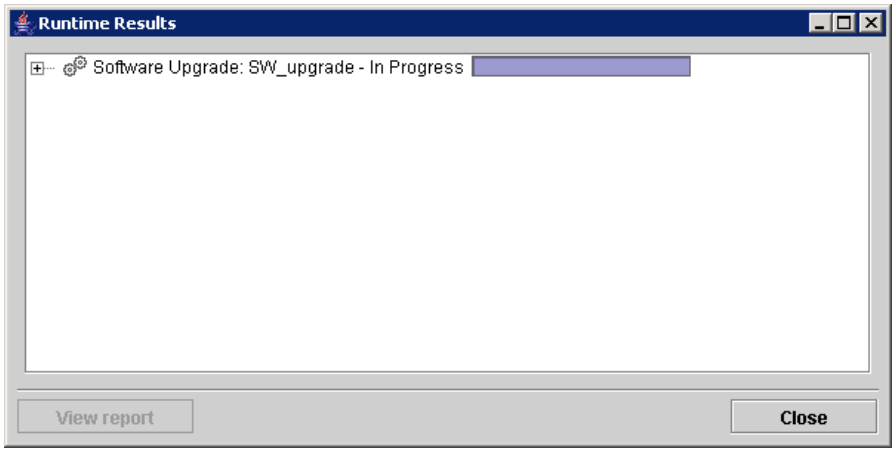

Figure 5-15: Software Upgrade Task - Runtime Results

If the task is Inactive, the Software Upgrade Task window is displayed.

Figure 5-16: Software Upgrade Task Window

The Software Upgrade Task window includes two tabs:

- ◇ “General Tab” - Section 5.2.8.1
- ◇ “Equipment Tab” - Section 5.2.8.2

2 Edit the parameters as required and click **OK** to save the changes and close the task window, *Cancel* to close the window without saving, or **Run** the execute the task. The adjacent field display changes from Inactive to Active, until the task has completed. When completed, you can view the report from the Task Editor or from the Task Manager.

5.2.8.1 General Tab

The General tab of the Software Upgrade Task window comprises the following fields:

Parameter	Description
Name	The name of the task. A string of up to 255 printable characters. The name must be unique in the system. This field is read-only when modifying an existing task.
Operations	
File Name	Select the upgrade file from the list (for BS NPU, Micro BS, AU, and/or SU).
Operation	The actions to take place once the new software file is loaded into the devices. Select from the following options: ■ *Load to Shadow* (NPU/µBST) - Loads the upgrade file to the Shadow memory of the applicable device(s). ■ *Load to BS* (AU/SU) - Loads the upgrade file to the NPU/µBST. ■ *Set as Main* - Performs the Load to Shadow operation, then resets the device(s) and boots them from the Shadow file, swaps the files and sets the running file as the new Main file.
Defaults	
Set SU Defaults	Temporary SUs cannot be selected directly for SW upgrade. Check to set the File Name and Operation of SUs as the default File Name and default operation of temporary SUs.
File Management Policy	

Parameter	Description
If space is needed in BS	Defines the policy to be used when the maximum number of software upgrade files is reached. Select from the following options: ■ Delete oldest files - deletes the oldest file to make room for the new file ■ Skip BS - the software upgrade file will not be loaded to the Base Station and the software upgrade task will skip the Base Station.
If BS running from Shadow	If a Base Station is running from the shadow version, the software upgrade task can either skip the Base Station or set the currently running shadow version as the main version. This option runs before any operation.

5.2.8.2 Equipment Tab

The Equipment tab enables to select equipment for the Software Upgrade task. The task will run on the selected equipment only.

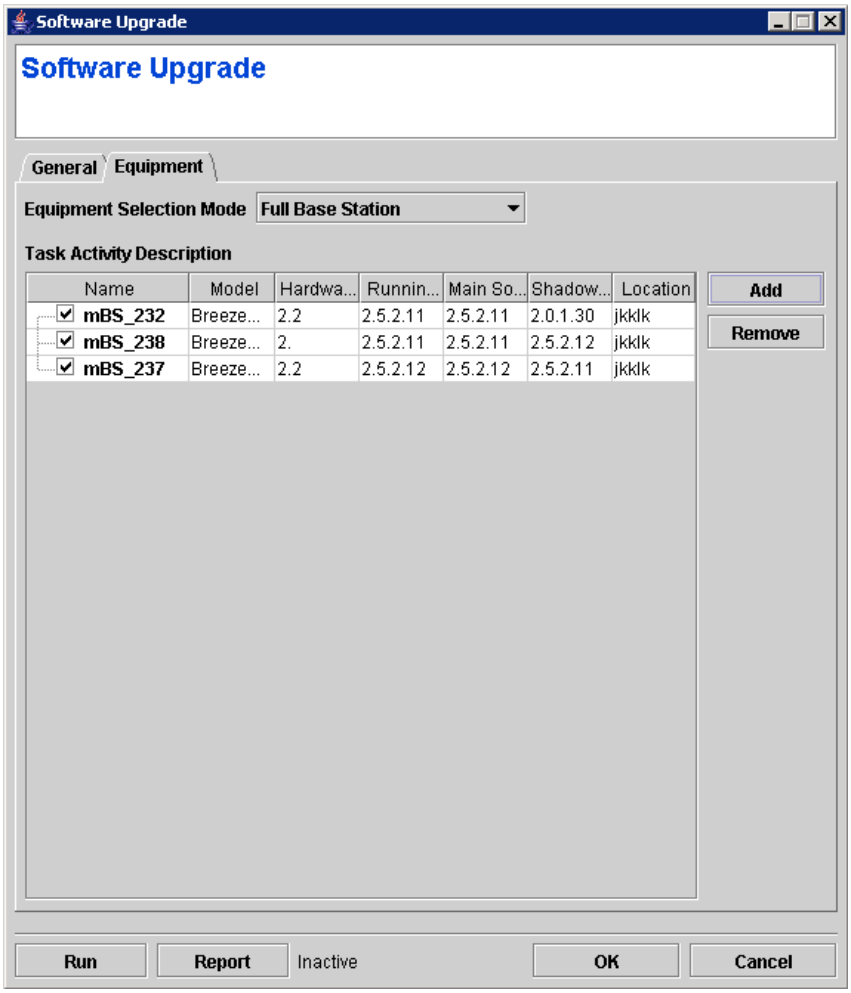

Figure 5-17: Software Upgrade Task - Equipment Tab

To add equipment to the list:

1 Select the Equipment Selection Mode:

- Full Base Station - enables to select Base Stations/Micro Base Stations only. All connected SUs and all connected AUs will be upgraded according to configured task policies.
- Individual Network Components - enables to select individual components: *NPUs/Micro Base Stations*, *AUs*, and/or *SUs*.

2 Click **Add**.

- If Full Base Station was selected in step 1 above, the Select Equipment window opens, listing all available Base Stations.
- If Individual Network Components was selected in step 1 above, a sub-menu opens, allowing you to: Select NPUs/MBSs, AUs, or SUs. Select one of the options. The Select Equipment window opens, listing all available equipment according to your selection.

3 Select the required equipment from the list. Use the Ctrl or Shift keys to select more than one unit and click **Select**. The selected equipment are displayed in the list.

4 Click **OK** to confirm your changes and close the window, or *Cancel* to close the window without saving your changes.

To remove equipment from the list:

1 Select the equipment to be removed from the list. Use the Ctrl or Shift keys to select more than one unit.

2 Click **Remove**. The unit is deleted from the list.

3 Click **OK** to confirm your changes and close the window, or *Cancel* to close the window without saving your changes.

5.2.8.3 The Software Upgrade Process

This section describes a complete SW upgrade process for all components of the cells: NPUs/Micro Base Stations, AUs, and permanent SUs.

The SW upgrade process is performed automatically in stages:

Stage 1: Uploads

1 Upload the selected file to the NPU's/Micro Base Station's Shadow:

a If the NPU is currently running from Shadow, the File Management policy is applicable:

1 "If BST is running from Shadow = Set as main", then a command for SET AS MAIN will be sent and the process will start from Step 1.1.

2 "If BST is running from Shadow = Skip BS" then the NPU will be ignored.

b If the NPU is currently running from Main, the load to shadow operation will be performed.

2 Upload AU/SU files to NPU/Micro Base Station.

Before uploading, the File management policy will be checked:

a If Delete, delete oldest file and replace it with the new file.

b If Skip BS, the upgrade procedure will be skipped.

3 Upload AU/SU files to AU/SU's shadow:

a If the AU/SU is currently running from Shadow then a command for SET AS MAIN will be sent and the process will start from Step 1.3.

b If the AU/SU is currently running from Main, the load to shadow operation will be performed.

Step 2: upgrading SUs stage

Before upgrading the SUs, the following conditions will be checked:

1 If the SU is registered:

a If the version already exists as the Main version in the SU, then the result will be "Already running".

b If the SU is currently running from Shadow, then a command for SET AS MAIN will be sent and the process will start from Step 1.3.

c If none of the conditions above is met, the SET AS MAIN command will be sent.

2 If the SU is not registered then the result will be Skipped with a failure: "SU.<mac address> is not registered"

Each of these conditions will be checked for batches of 5 SUs, during the SW upgrade and for 5 minutes.

Step 3: upgrading AUs stage

Before upgrading the AUs, the following conditions will be checked:

1 If the AU is connected:

a If the version already exists as the Main version in the AU, then the result will be "Already running".

b If the AU is currently running from Shadow, then a command for SET AS MAIN will be sent and the process will start from Step 1.3.

c If none of the conditions above is met, the SET AS MAIN command will be sent.

2 If the AU is not registered, then the result will be Skipped with a failure: “AU.<id> is not connected”

Each of these conditions will be checked, during the SW upgrade and for 5 minutes.

Step 4: upgrade the NPU

1 If the version already exists as the Main version in the NPU, then the result will be Skipped - “Already running”.

2 If the NPU is currently running from Shadow, the File management policy is applicable:

a “If BST is running from Shadow = Set as main”, then a command for SET AS MAIN will be sent.

b “If BST is running from Shadow = Skip BS”, then the NPU will be ignored.

3 If none of the conditions above is met, the SET AS MAIN command will be sent.

In addition, a SET command for SU default file will be sent.

5.2.9 BreezeMAX Configuration Backup Task

The Configuration Backup Task enables to create backup files of the Base Station configuration. The backup file contains copies of all the applicable configuration files and databases in the system.

To open the Configuration Backup Task window:

1 In the Task Manager window:

◇ Click **New**, select **BreezeMAX Configuration Backup** from the list of available task types and click **OK**. The Configuration Backup Task window is displayed.

OR

◇ Select an existing Configuration Backup task from the list and click **Modify**. If the task is Active, the Runtime result screen is displayed, displaying the status of the running task.

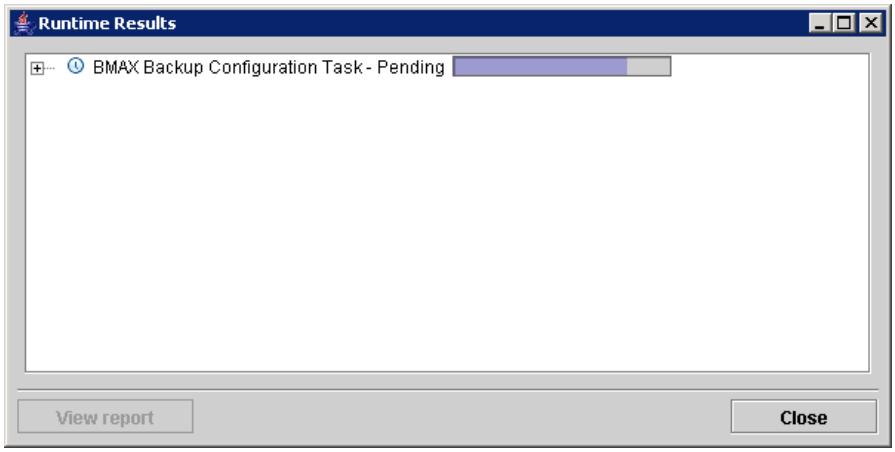

Figure 5-18: Configuration Backup Task - Runtime Results

If the task is Inactive, the Configuration Backup Task window is displayed.

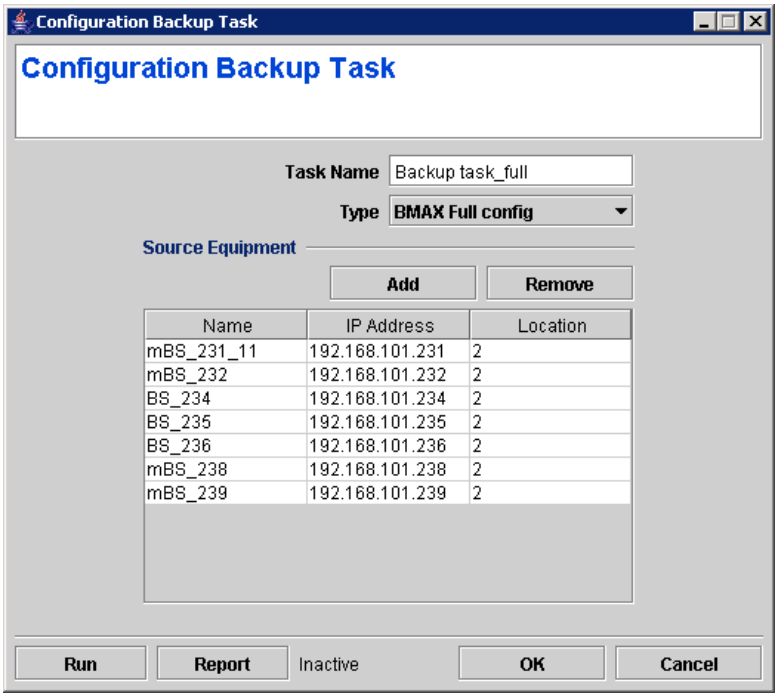

Figure 5-19: Configuration Backup Task Window

Alternatively, the Configuration Backup Task window can also be accessed from the Equipment Manager. In the Equipment Manager, select a device and click on **Backup Configuration**.

The Configuration Backup Task window comprises the following fields:

Parameter	Description
Task Name	The name of the task. A string of up to 255 printable characters. The name must be unique in the system. This field is read-only when modifying an existing task.
Type	The type of backup file: ■ Full config: The entire Base Station configuration (excluding Passwords and basic IP parameters of the MGMT and DATA ports - IP Address, Subnet Mask and Default Gateway). ■ Service Profile: All the profiles associated with services (Service Profiles, Forwarding Rules, Priority Classifiers, QoS Profiles). ■ Services: All the profiles and configurations associated with service (Subscribers, Services, Service Profiles, Forwarding Rules, Priority Classifiers, QoS Profiles). ■ Traps: The configuration parameters for all traps. ■ Filters: All the configurations of Filtering Rules, Interface Filtering and MAC Address Deny List.

2 Click **Add**. The Equipment selection window is displayed, enabling to select the Base Station(s) for which to perform the configuration backup. Click **Remove** to delete the selected Base Station from the list.

3 Click **OK** to save the changes and close the task window, **Cancel** to close the window without saving, or **Run** to execute the task. The adjacent field display changes from Inactive to Active, until the task has completed. When completed, you can view the report from the task window or from the Task Editor or from the Task Manager.

5.3 License Manager

The License Manager displays information about valid licenses for managing Alvarion devices and summary details on the currently managed device types, included in the license.

To open the License Manager window:

Select *System Utilities* > *License Manager* from the *File* > *Open* > *AlvariSTAR* menu or the Navigation Pane.

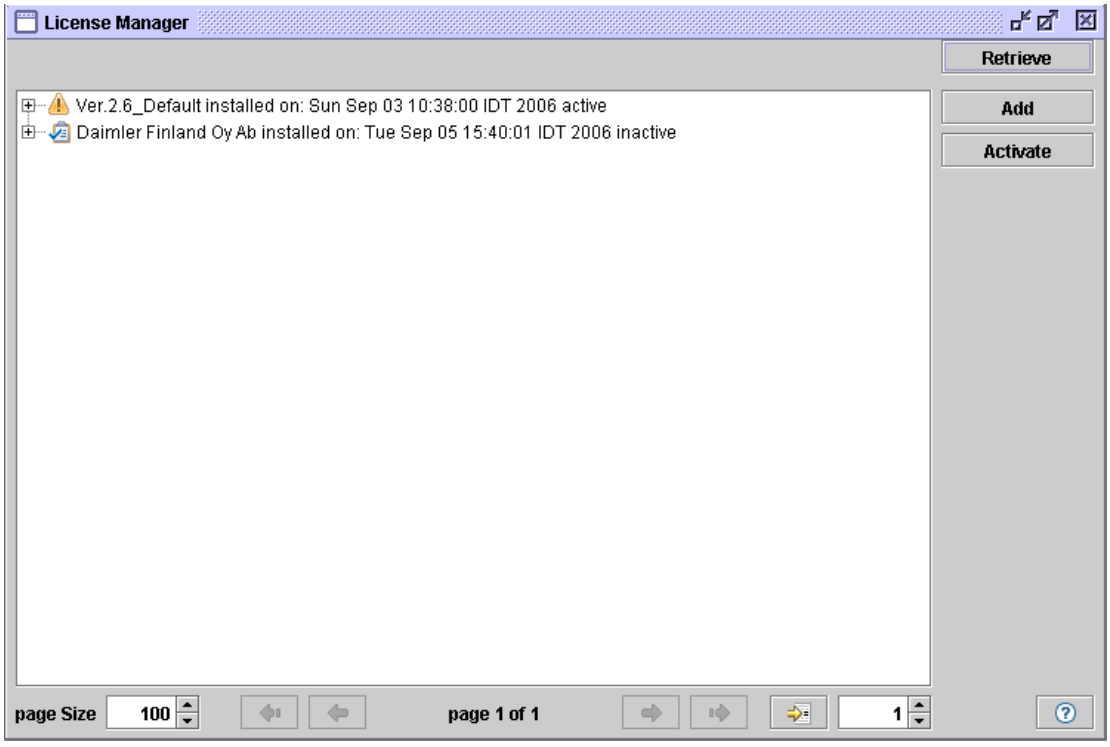

Figure 5-20: License Manager

The License Manager displays the following information for each licensed device type: <Name> (#) used: #

Parameter	Description
Name	The device type: BreezeMAX BS, BreezeMAX SU, BreezeMAX MBS.
(#)	The number of licensed devices of the applicable type.

Parameter	Description
used: #	The number of managed devices. The number increases whenever a new device is discovered.

When the number of discovered devices (Managed Devices) reaches the number of Licensed Devices, additional discovered devices will be ignored.

Unlicensed devices will be marked in Equipment Manager with an exclamation icon.

When considering future expansion plans, the number of licensed devices compared with the number of managed devices of each type, will indicate whether there is a need for an updated license.

5.3.1 Adding Licenses

Before adding a license, make sure that the file obtained from the supplier is available.

To add licenses:

Click **Add** and browse to the location of the license file. Select the file and click **Open**. The new licenses are displayed on the list. Alternatively, save the license file in the /AlvariSTAR/filesystem/license folder. The next time the server will be restarted, the new license will also be added.

5.3.2 Activating Existing Licenses

The new license added to the AlvariSTAR system, needs to be activated in order to enable AlvariSTAR to manage the required devices.

To activate a license:

Select the required license and click on **Activate**.

NOTE

Activating a license will deactivate all other licenses.

5.4 User Monitor

The User Monitor window displays information on the currently logged in users and enables sending messages to a logged in user. Users with Administrator rights can terminate the application of other users.

To open the User Monitor:

Select *System Utilities* > *User Monitor* from the *File* > *Open* > *AlvariSTAR* menu or the Navigation Pane. The User Monitor displays a list of currently logged in users.

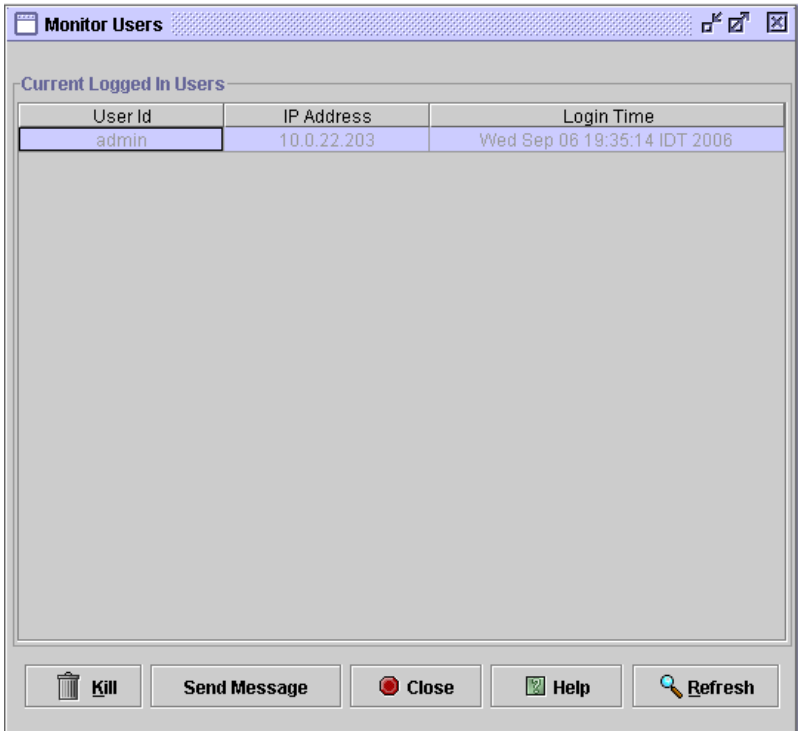

Figure 5-21: User Monitor Window

The *Current Logged In Users* table displays the User Id, IP address and login time for each of the currently logged in users.

In addition to the standard Close, Help and Refresh button, the following buttons are also available:

Parameter	Description
Send Message	Click after selecting one of the logged in users to open the Sending Message window, enabling you to send a short message to the selected user(s).
Kill	Click to terminate the application of a selected user. Only an Administrator can perform this operation to terminate applications of users with lower permission levels.

5.5 Audit Logs

AlvariSTAR provides a logging service that records messages to the database upon the occurrence of pre-specified events. These messages can include event date and time, event type, error messages and other important information according to the recorded event. The Audit Log Manager enables to view recorded events and export the logged data to an external Comma Separated Value (CSV) file.

To open the Audit Log Manager:

Select *System Utilities* > *Audit Logs* from the *File* > *Open* > *AlvariSTAR* menu or the Navigation Pane. The Audit Log Manager displays a list of all logged records.

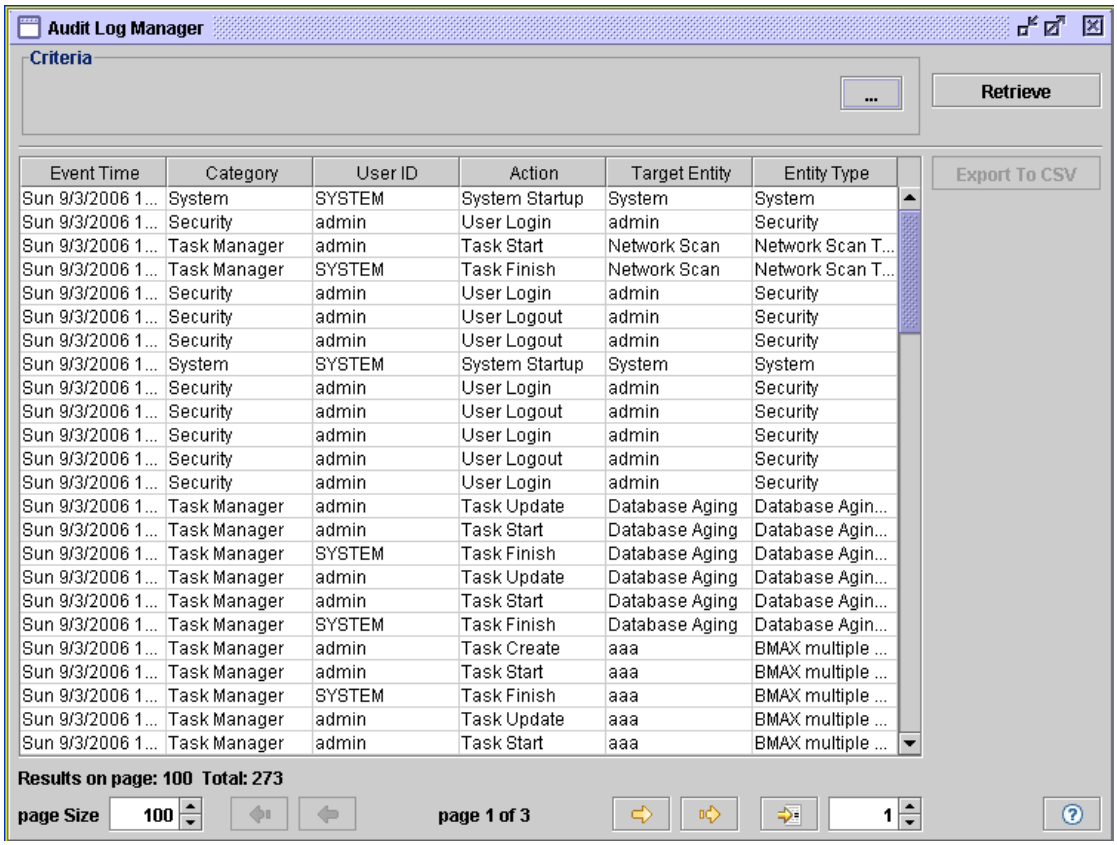
Audit Log Manager
Criteria
...
Retrieve
Export To CSV
Event Time | Category | User ID | Action | Target Entity | Entity Type
Sun 9/3/2006 1... | System | SYSTEM | System Startup | System | System
Sun 9/3/2006 1... | Security | admin | User Login | admin | Security
Sun 9/3/2006 1... | Task Manager | admin | Task Start | Network Scan | Network Scan T...
Sun 9/3/2006 1... | Task Manager | SYSTEM | Task Finish | Network Scan | Network Scan T...
Sun 9/3/2006 1... | Security | admin | User Login | admin | Security
Sun 9/3/2006 1... | Security | admin | User Logout | admin | Security
Sun 9/3/2006 1... | Security | admin | User Logout | admin | Security
Sun 9/3/2006 1... | System | SYSTEM | System Startup | System | System
Sun 9/3/2006 1... | Security | admin | User Login | admin | Security
Sun 9/3/2006 1... | Security | admin | User Logout | admin | Security
Sun 9/3/2006 1... | Security | admin | User Login | admin | Security
Sun 9/3/2006 1... | Security | admin | User Logout | admin | Security
Sun 9/3/2006 1... | Security | admin | User Login | admin | Security
Sun 9/3/2006 1... | Task Manager | admin | Task Update | Database Aging | Database Agin...
Sun 9/3/2006 1... | Task Manager | admin | Task Start | Database Aging | Database Agin...
Sun 9/3/2006 1... | Task Manager | SYSTEM | Task Finish | Database Aging | Database Agin...
Sun 9/3/2006 1... | Task Manager | admin | Task Update | Database Aging | Database Agin...
Sun 9/3/2006 1... | Task Manager | admin | Task Start | Database Aging | Database Agin...
Sun 9/3/2006 1... | Task Manager | SYSTEM | Task Finish | Database Aging | Database Agin...
Sun 9/3/2006 1... | Task Manager | admin | Task Create | aaa | BMAX multiple ...
Sun 9/3/2006 1... | Task Manager | admin | Task Start | aaa | BMAX multiple ...
Sun 9/3/2006 1... | Task Manager | SYSTEM | Task Finish | aaa | BMAX multiple ...
Sun 9/3/2006 1... | Task Manager | admin | Task Update | aaa | BMAX multiple ...
Sun 9/3/2006 1... | Task Manager | admin | Task Start | aaa | BMAX multiple ...
Results on page: 100 Total: 273
page Size
100
page 1 of 3
1

Figure 5-22: Audit Log Manager

For each audit record, the following information is displayed:

Field	Description
Event Time	The date and time of the event.
Category	The category of the event. See Table 5-1.
User ID	The user who initiated the action. System User ID indicates a system initiated action.
Action	The action performed. See Table 5-1.
Target Entity	The entity associated with the event.
Entity Type	The type of entity associated with the event. See Table 5-1.

Table 5-1: Available Entities

Category	Action	Entity Type
Security	■ User Login ■ User Logout	Security
Task Manager	■ Task Create ■ Task Update ■ Task Delete ■ Task Start ■ Task Finish ■ Task Schedule ■ Task Unschedule ■ Task Abort	■ Database Aging Task ■ Configuration Restore ■ Multiple SU Configuration ■ Single Range Scan Task ■ Configuration Backup ■ Software Upgrade ■ Network Scan Task ■ Service Profile Distribution ■ Performance Collection Task ■ Multiple BS Configuration
Equipment Management	■ Equipment Create ■ Equipment Delete	■ BreezeMAX BS ■ BreezeMAX MBS ■ BreezeMAX SU
System	■ System Startup ■ System Shutdown	System

Table 5-1: Available Entities

Category	Action	Entity Type
License	■ License Imported ■ License Activated ■ License Expired	License

To export the information of selected audit records:

Click to export, browse to the desired location, enter a file name, and click **Save**.

6

Chapter 6 - Event Services

In This Chapter:

- "Event Services" on page 166
- "Event Monitor" on page 167
- "Event History" on page 170
- "Managing Alarms" on page 172
- "Event Template Manager" on page 182
- "Northbound Manager" on page 198
- "Event View Manager" on page 206
- "Event Filter Manager" on page 211
- "Command Manager" on page 218

6.1 Event Services

The Event Services feature comprises efficient tools for managing alarms generated in the system. Information about each alarm is readily displayed, helping operators diagnose and correct system failures. The Event Services tools allow you to acknowledge received alarms, clear, or forward them. You can apply filters to display specific alarms or to display specific information about each alarm according to your needs.

You can connect to other management systems and forward traps, apply templates to automate the processing of alarms, and trigger external scripts.

The following Event Services tools are available:

- Event Monitor - Displays real time updates of new alarms entering the system, color coded according to severity and allows to manage each alarm.
- Event History - Displays a list of all alarms that occurred in the system, color coded according to severity.
- Event Template Manager - Allows to create, edit and delete templates to automate the processing of alarms.
- Northbound Manager - Provides an interface where you can connect to other management systems and effectively forward traps.
- Event View Manager - Allows to manipulate the information displayed for alarms.
- Event Filter Manager - Allows to create, edit and delete filters to display alarms according to user-defined criteria.
- Command Manager - Allows to associate template-matched alarms with external scripts.

6.2 Event Monitor

The Event Monitor window displays real time updates of new alarms entering the system, or alarms created from the window launch time, color coded according to severity. It allows you to manage and diagnose alarms.

To open the Event Monitor:

Select *Event Services* > *Event Monitor* from the *File* > *Open* menu or from the Navigation Pane. The Event Monitor window is displayed:

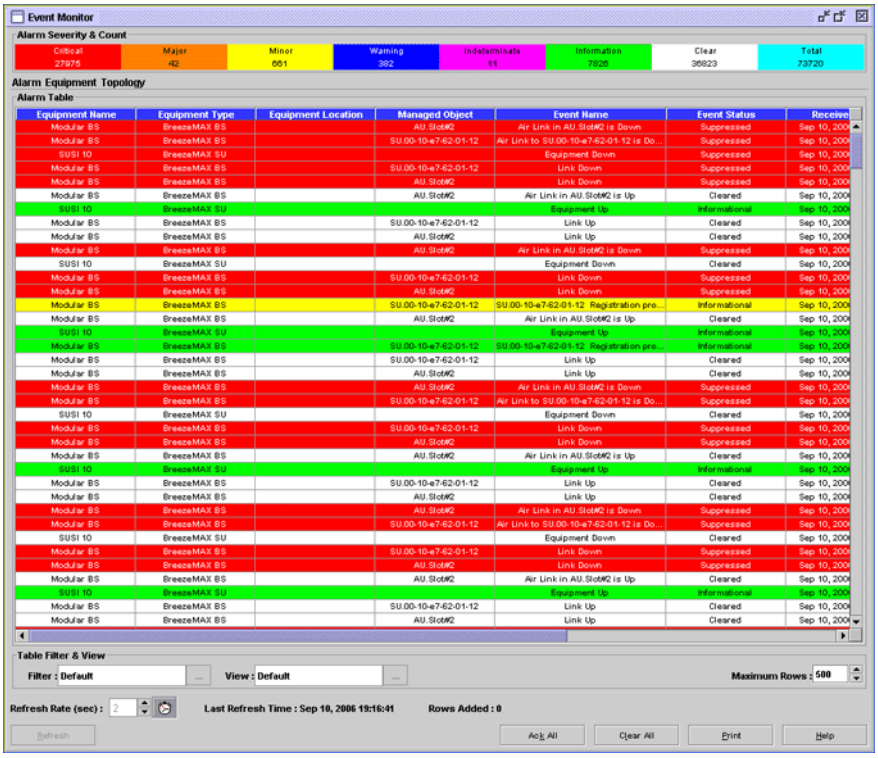

Figure 6-1: Event Monitor Window

When the Event Monitor is launched, it opens in Listening mode. The display is updated whenever an alarm is received or cleared.

The Event Monitor window is divided into the following main areas:

- *Alarm Severity & Count* - displays the list of severities, color coded according to pre-defined settings, and a count of active alarms distributed according to

severity. The count of active alarms will not be displayed for filtered out alarms. It also displays the total number of the active alarms that have not been filtered out.

- *Alarm Table* - displays general information about each alarm (see Section 6.4.1). You can customize the information displayed in the table to provide a more efficient view. You can also define the maximum number of alarms displayed in the table (see Section 6.4.1.1).

- *Table Filter and View* - allows you to select a filter and view from the drop-down menus. To change the filter or view, deactivate the *Refresh Rate Manager*. Refer to Section 6.7 and Section 6.8 for information on how to create and edit view and filter options.

- *Refresh Rate (sec)* - enables to set the rate at which the screen refreshes. Click on the clock icon to the right of the field to activate/deactivate automatic refreshing and enables to change the refresh rate. Deactivating the timer stops the automatic refreshing. New alarms are collected but not displayed. To view updates, reactivate the timer, or click on the **Refresh** button to manually refresh the display.

- *Last Refresh Time* - a read-only display of the last time either an automatic or manual refresh occurred.

- *Rows Added* - a read only display of the number of rows added with the last refresh.

- *Maximum Rows* - Allows you to limit the number of displayed alarms. See Section 6.4.1.1.

- Control Buttons - See Section 6.4.5.

Section 6.4 provides details on managing alarms in the Event Monitor and Event History. The following information is available:

- "Alarm Table," Section 6.4.1

- "Alarm Severities," Section 6.4.2

- "Alarm Details Window," Section 6.4.3

- "Alarm Operations," Section 6.4.4

- “Control Buttons,” Section 6.4.5

6.3 Event History

The Event History window displays a list of all alarms and alarms occurred in the system, color-coded according to severity. A total of uncleared alarms, listed both by category and in sum, appears at the top of the Event History window.

To open the Event History:

Select *Event Services* > *Event History* from the *File* > *Open* menu or from the Navigation Pane. The Event History window is displayed:

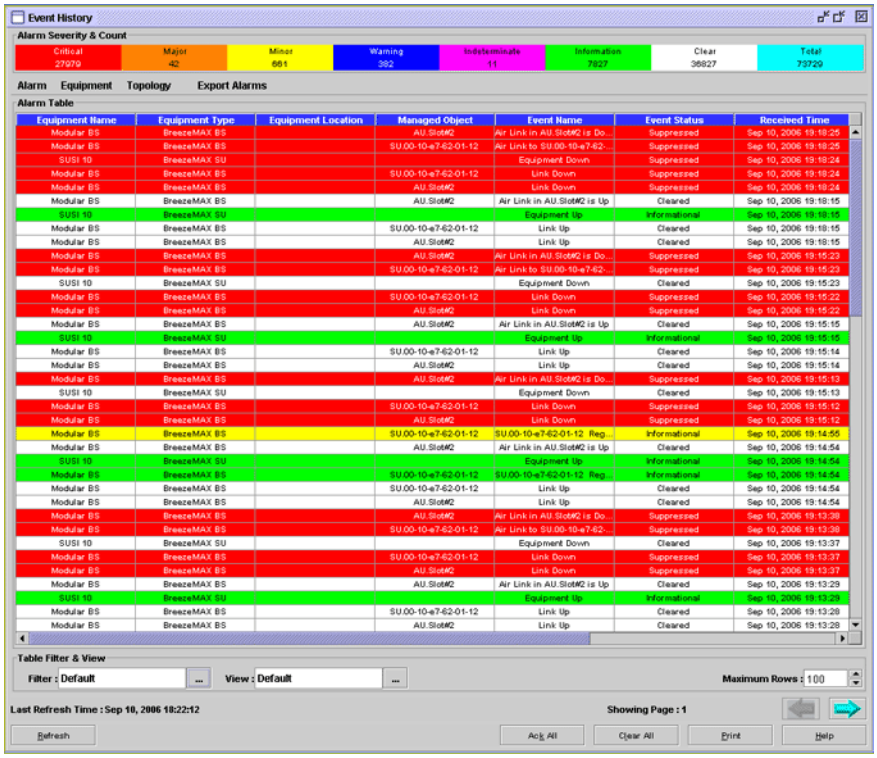

Figure 6-2: Event History Window

To display newly received alarms or to updated the display of cleared alarms, you need to click on the **Refresh** button.

The Event History window is divided into the following main areas:

- *Alarm Severity & Count* - displays the list of severities, color coded according to pre-defined settings, and a count of active alarms distributed according to

severity. The count of active alarms will not be displayed for filtered out alarms. It also displays the total number of the active alarms that have not been filtered out

- *Alarm Table* - displays general information about each alarm (see Section 6.4.1). You can customize the information displayed in the table to provide a more efficient view. You can also define the maximum number of alarms displayed in the table (see Section 6.4.1.1).
- *Table Filter and View* - allows you to select a filter and view from the drop-down menus. Refer to Section 6.7 and Section 6.8 for information on how to create and edit view and filter options.
- Maximum Rows - allows you to limit the number of displayed alarms. See Section 6.4.1.1.
- *Last Refresh Time* - a read-only display of the last time either an automatic or manual refresh occurred.
- *Showing page* - a read only display of the number of the page displayed. You can browse through the multiple screen displays using the right/left arrows.
- Control Buttons - See Section 6.4.5.

Section 6.4 provides details on managing alarms in the Event Monitor and Event History. The following information is available:

- "Alarm Table," Section 6.4.1
- "Alarm Severities," Section 6.4.2
- "Alarm Details Window," Section 6.4.3
- "Alarm Operations," Section 6.4.4
- "Control Buttons," Section 6.4.5

6.4 Managing Alarms

The following paragraphs describe how to manage alarms using the Event Monitor and Event History.

6.4.1 Alarm Table

The Alarms Table presents general information about each alarm occurred in the system. You can change the displayed attributes (columns) through the View Manager (see Section 6.7).

The following describes the available attributes (columns) in alphabetic order.

Parameter	Description
Ack By	The user who acknowledged the alarm.
Ack Time	The date and time the alarm was acknowledged.
Clear By	The user who cleared the alarm.
Clear Cause	The reason for clearing the alarm.
Clear Time	The date and time that the alarm was cleared.
Community String	The SNMP community of this alarm.
Enterprise Trap/OID	The trap value.
Equipment Location	The location of the equipment at the source of the alarm.
Equipment Name	The name of the equipment at the source of the alarm.
Equipment Type	The type of equipment at the source of the alarm.
Event Name	The name of the alarm. For SNMP traps, the name is the trap OID. If the name is blank when received by the application, the alarm takes the name of the event template used for processing.
Event Status	The current status of the alarm. It can be Open, Cleared, or Informational.
Event Type	The classification type of the alarm. The alarm types are: All, Security Alarm, Alarm, Informational.
Icon	A graphic image that indicates the alarm's severity.
Last Update Time	The date and time the network element last updated the alarm.
Managed Object	The name of the equipment associated with the alarm. If the object name is unknown, NotFound appears. An identification of a component of the network element for which the alarm occurred. For example a port on a router would be a managed object instance.
Mediation Agent	The IP address of the mediation agent reporting this alarm.

Parameter	Description
Protocol	The protocol used to send and receive the alarm. Valid protocols are: SNMP v1, SNMP v2, Q3, and Other.
Received Time	The time the alarm was received by a mediation agent.
Service Affecting Alarm	Indicates if the alarm affects a service.
Severity	The severity of the alarm. The severity only has meaning for Alarms and Security Alarms. Informational Alarms get a severity level of Indeterminate.
Source	The IP address of the object or device that sent the alarm. For Q3, the source is the TNS name of the device or object.
Specific	A unique identifier for an enterprise trap (Generic is 6). Specific defines what type of trap it is.
Value	The SNMP describes the trap value of the alarm.
Version	The SNMP version number.

6.4.1.1 Limiting the Number of Alarms Displayed

You can define the maximum number of alarms to be displayed in the table by entering a number in the *Maximum Rows* box or by using the up and down arrows to the right of the number field. The range for both Event History and Event Monitor is 1 to 1000.

If the maximum number of alarms is displayed, older alarms will be removed from the list to make room for new received alarms. The older alarms are not deleted from the database, only from the display.

6.4.1.2 Customizing Views in Event Monitor / Event History

You can make changes to a view by adjusting columns in the Alarm Table.

The following are the available options for customizing the view:

- Sort columns - Click on the column header of the column according to which you want to sort the table. An icon appears on the header, indicating sorting in ascending/descending order.

NOTE

No column sorting is available in the Event Monitor.

- Move Columns - Click the column header of the column you want to move and drag it to its new location.

- Resize Columns - Click the right margin of the column header you want to resize and drag to resize the column. The column margin is located between the column headers.

NOTE

To save the changes for future sessions, you need to save your changes as a view (see Section 6.7).
Column size cannot be saved.

You can also:

- Remove/insert columns using the Event View Manager (see Section 6.7)
- Configure which alarms will appear in the Alarm Table, using the Event Filter Manager (see Section 6.8).

6.4.2 Alarm Severities

AlvariSTAR is delivered with a set of default alarm severity definitions, each with its own default color.

The default severity definitions are:

Parameter	Description
Critical	A service-halting condition occurs, requiring immediate corrective action. The equipment is completely out of service and you must restore its capability.
Major	A service-affecting condition has developed and corrective action is required. There is severe degradation in the equipment's capability and you must restore its full capability.
Minor	A non-service-affecting fault condition exists and corrective action should be taken in order to prevent a more serious fault. The detected alarm condition is not currently degrading the capacity of the equipment.
Warning	A potential or impending service-affecting fault could occur, and no significant effects have yet been felt. Action should be taken to further diagnose and correct the problem to prevent it from becoming a more serious service-affecting fault. The detected alarm condition does not currently pose a problem, but may degrade the capacity of the equipment if you do not take corrective action.
Indeterminate	The severity level cannot be determined.

Parameter	Description
Information	General information about the condition of the object, device, or system.
Cleared	The problem is corrected, and the correlated alarm is cleared from the Alarm Table.

6.4.3 Alarm Details Window

The Alarm Tables in the Event Monitor/Event History provide a simplified display, summarizing each alarm. The Alarm Details window, however, presents all the information associated with a selected alarm.

To open the Event Detail Information window:

From the Event Monitor/Event History window, select an alarm from the table, right-click and select **Alarm Details** from the *Alarm* pop up menu, or from the Alarm menu above the Alarm Table. You can also double-click on the alarm.

An example of the Alarm Details window is displayed below:

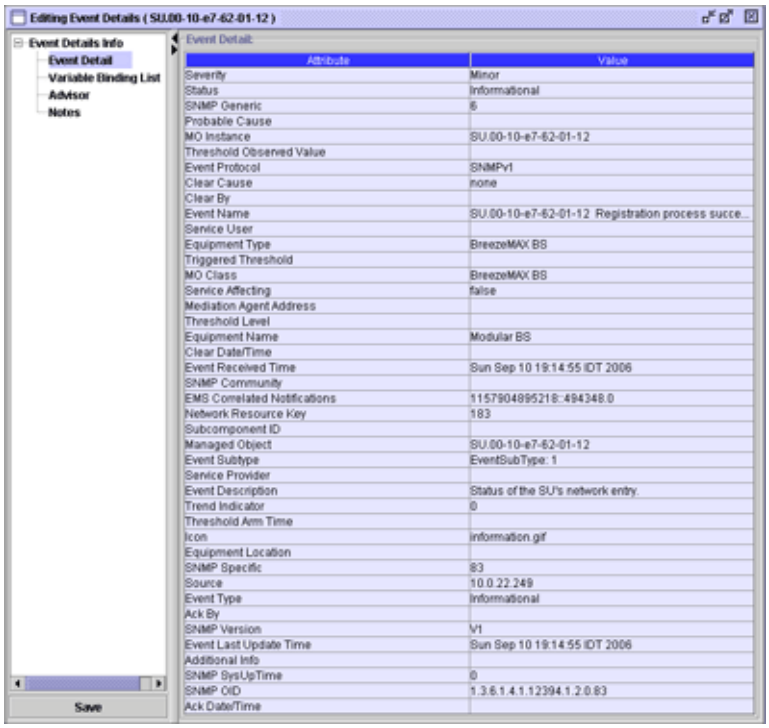

Figure 6-3: Alarm Details Window

The Alarm Details window consists of the following pages:

- "Event Detail Page," Section 6.4.3.1
- "Variable Binding List Page," Section 6.4.3.2
- "Advisor Page," Section 6.4.3.3
- "Notes Page," Section 6.4.3.4

6.4.3.1 Event Detail Page

Double click on an event to open the Event Details page. The Event Detail page displays the same alarm attributes as the Alarm Tables in Event Monitor/Event History (see Section 6.4.1), and the following additional attributes:

Parameter	Description
Ack By	The user who acknowledged the alarm.
Ack Date/Time	The date and time the alarm was acknowledged.
Additional Info	Additional information about the alarm.
Clear By	The user who cleared the alarm.
Clear Cause	The reason for clearing the alarm.
Clear Date/Time	The date and time that the alarm was cleared.
EMSCorrelated Notifications	Element Management System notification identifier correlated with this alarm. For example, when a linkDown alarm comes into the system. Event Services assigns it a notification identifier number. If a linkUp alarm arrives, causing Event Services to clear the linkDown alarm, the linkDown notification identifier is placed into the EMSCorrelated Notification field of the linkUp alarm.
Equipment Location	The physical location of the equipment.
Equipment Name	The name of the equipment.
Equipment Type	The type of equipment: Base Station, Micro Base Station, SU, NPU, AU.
Event Description	An optional text description of the alarm as defined in the related event template.
Event Last Update Time	The date and time the Alarm Table was last updated.
Event Name	The name of the alarm. For SNMP traps, the name is the trap OID. If the name is blank when received by the application, the alarm takes the name of the event template used for processing.
Event Protocol	The protocol that sends and receives the alarm. Valid protocols are: SNMP v1, SNMP v2, Q3, and Other.

Parameter	Description
Event Received Time	The time a mediation agent received the alarm.
Event Sub Type	The Event Sub Type further defines the Event Type. The available event sub types depend on the selected event type. The event sub types are: ■ Alarm - Indeterminate, Communications alarm, Quality of Service alarm, Processing error alarm, Equipment alarm, Environmental alarm ■ Security Alarm - Indeterminate, Integrity violation, Operational violation, Physical violation, Security service or mechanism violation, Time domain violation ■ Informational Alarm - Indeterminate
Event Type	The classification type of the alarm. Event types are: ■ All ■ Security Alarm ■ Alarm ■ Informational
Icon	An image that indicates the alarm's severity.
Managed Object	The name of the equipment associated with the alarm. If the object name is unknown, NotFound appears.
MO Class	The class of the equipment that sent the alarm. For example, the equipment is classified as a server and grouped into the com.ngnms.products.vl.common.AlvariSTAR_VL_AU class in the Equipment Manager.
MO Instance	A specific instance of the Managed Object Class.
Mediation Agent Address	The IP address of the mediation agent that received the trap.
Network Resource Key	The key of the equipment class object representing the network element in the Oware Management Center BOM.
Probable Cause	The probable cause of the alarm.
Service Affecting	Indicates if the alarm affects a service.
Service Provider	The service provider of the service that led to the generation of the alarm.
Service User	The service user whose request led to the generation of the alarm.
Severity	The severity of the alarm. The severity only has meaning for Alarms and Security Alarms. Informational Alarms get a severity level of Indeterminate.

Parameter	Description
SNMP Community	The SNMP read-write community of the object. Values are either Public or Private. For Q3, the value is always Public.
SNMP OID	The SNMP Object Identification number. For SNMP v1, the OID the enterprise value from the SNMP PDU. For SNMP v2c, the OID is the SNMP trap OID. For Q3, the OID is the Q3 Alarm Enterprise OID—1.3.6.1.4.1.231.7.1.3.1.1.5.204.
SNMP Specific	The specific trap code as defined in the MIB, used only if Generic trap is 6.
SNMP SysUpTime	Seconds elapsed since the object or device last rebooted. For Q3, it is seconds elapsed since the Q3 Listener/Parser last rebooted.
SNMP Generic	The generic trap code. For Q3, it indicates an enterprise specific trap.
SNMP Version	The SNMP version number
Source	The IP address of the object or device that sent the alarm. For Q3, the source is the TNS name of the device or object.
Status	The current status of the alarm. It can be Open, Cleared, or Informational.
SubComponent ID	A unique identifier for a subcomponent of the associated network element to the alarm.
Threshold Arm Time	The time at which the threshold was last re-armed for gauge thresholds. For counter thresholds, the time is either the last time the threshold offset was applied or the last time the counter was initialized.
Threshold Level	The value of the crossed threshold. The value appears only when the alarm is the result of crossing a threshold.
Threshold Observed Value	The value of the gauge or counter when the threshold was crossed.
Trend Indicator	The current severity trend—more or less severe—of the equipment.
Triggered Threshold	Identifier of the threshold attribute that caused the alarm. The value appears only when the alarm is the result of crossing a threshold.

6.4.3.2 Variable Binding List Page

The Variable Binding List page (Figure 6-4) displays a list of the variable bindings for the selected alarm.

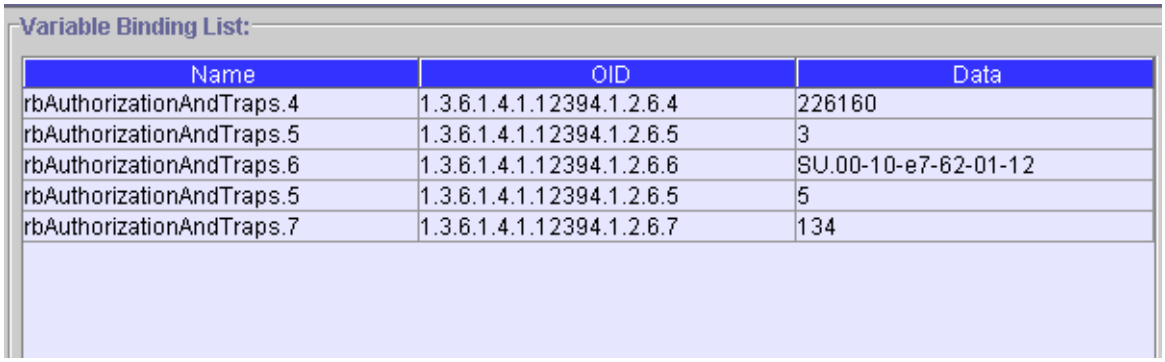

Figure 6-4: Variable Binding List

6.4.3.3 Advisor Page

The Advisor page displays a text description of the alarm and sometimes proposes a remedy. For example, *"The device has received an improperly authorized protocol message. The message has been discarded."* The default message displayed in the Advisor page comes from the trap's MIB, but the message can be edited in the Event Template Editor Advisor page (see Section 6.5.1.1). The Advisor message is the default message for any e-mails sent about the alarm.

6.4.3.4 Notes Page

The Notes page lets an operator provide additional information about the selected alarm, such as steps already taken to correct the problem. The note is stored with the alarm.

6.4.4 Alarm Operations

AlvariSTAR provides many alarm management features allowing you to diagnose, troubleshoot, process, and clear alarms.

All general alarm operations are available through pop-up menus and through the menus located directly above the Alarm Table. Select an alarm from the table and right-click on it to display the context menu, or use the relevant menu option.

The following are the items:

Parameter	Description
Alarm	
Alarm Details	Displays detailed information about the selected alarm. See Section 6.4.3 for additional information.

Parameter	Description
Acknowledge Alarm	Acknowledges the selected *open* alarm(s). The current date and time appear in the *Ack Time* field, and the name of the currently logged-on user appears in the *Ack By* field. Available if the Event type of a selected entity is Alarm and is not acknowledged automatically by correlation mechanism.
Unacknowledge Alarm	Unacknowledges previously acknowledged selected alarm(s), and clears the entries in the *Ack By* and *Ack Time* fields. Available for the current user if the alarm was previously acknowledged by the current user.
Clear Alarm	Clears only *open* selected alarm(s). Alarms' status changes from *open* to *cleared*. The status of the alarm changes from *open* to *cleared*, but the alarm remains in the table. Available if the Event type of a selected entity is Alarm and is not acknowledged automatically by correlation mechanism.
Email Alarm	Sends the selected alarm, via e-mail, to another operator. You must enter the full e-mail address—for example, `johnq.user@networkserviceprovider.com`.
Remove Alarm	Available only in Event Monitor. Removes the selected alarm from the alarms current view.
Equipment	
Equipment Details	Opens the Configuration Manager for the selected equipment.
Cut Through	Opens a Telnet session to the device. Applicable only for devices that support this feature.
Topology	
Topology View	Displays the Location Map centered on the equipment associated with the selected alarm. Available only when the device has a location associated with it.
Export Alarms	Available only in Event History. Exports the selected alarm(s) and creates a comma delimited text file that can be imported into other programs (for example, a spreadsheet).

6.4.5 Control Buttons

In addition to the standard Close and Help buttons, Event Monitor and Event History windows include the following buttons:

Parameter	Description
Ack All	Allows you to acknowledge all open alarms.

Parameter	Description
Clear All	Allows you to clear all open alarms.
Refresh	Refreshes the display according to a selected *View*/*Filter*, and the *Maximum Rows* parameters. Available when the clock icon is not pressed.
Print	Prints the list of alarms.
Help	Opens the help for the Event Monitor/Event History.

6.5 Event Template Manager

Event Templates determine how AlvariSTAR processes different types of messages sent by managed network objects. These templates can even trigger external scripts (see Section 6.9). The system's messages (alarms) typically indicate a change in the operational status of the object, like a device failure or a system reset. Event templates match each incoming message with specific actions. Device drivers often install their own templates.

To open the Event Template Manager:

Select *Event Services* > *Event Template Manager* from the *File* > *Open* menu or from the Navigation Pane. The *Event Template Manager* window is displayed:

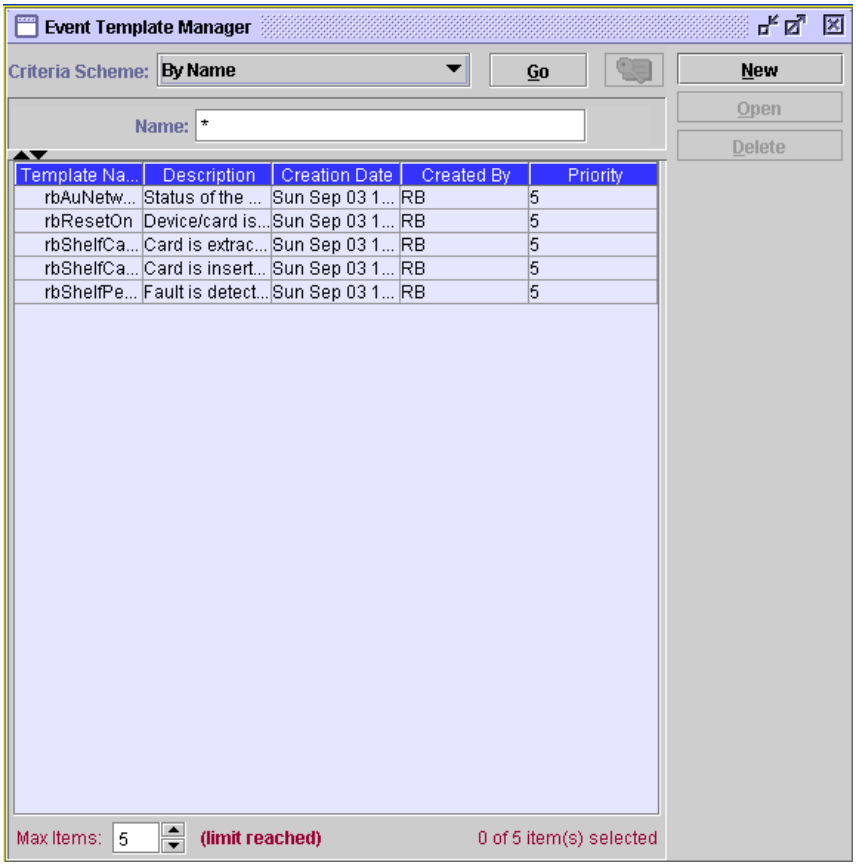

Figure 6-5: Event Template Manager

For each template, the following information is displayed:

Parameter	Description
Template Name	The name of the template.
Description	A description of the template.
Creation Date	The template's date of creation.
Created By	The user who created the template.
Priority	The template's priority. The range is 0~999999.

From the Event Template Manager you can:

- Create new event templates - Section 6.5.1
- Modify existing event templates - Section 6.5.2
- Delete event templates - Section 6.5.3
- Import event templates - Section 6.5.4

6.5.1 Creating Event Templates

To create a new event template:

1 From the Event Template Manager, click **New** to define a new event template. The Creating New Event Template window is displayed:

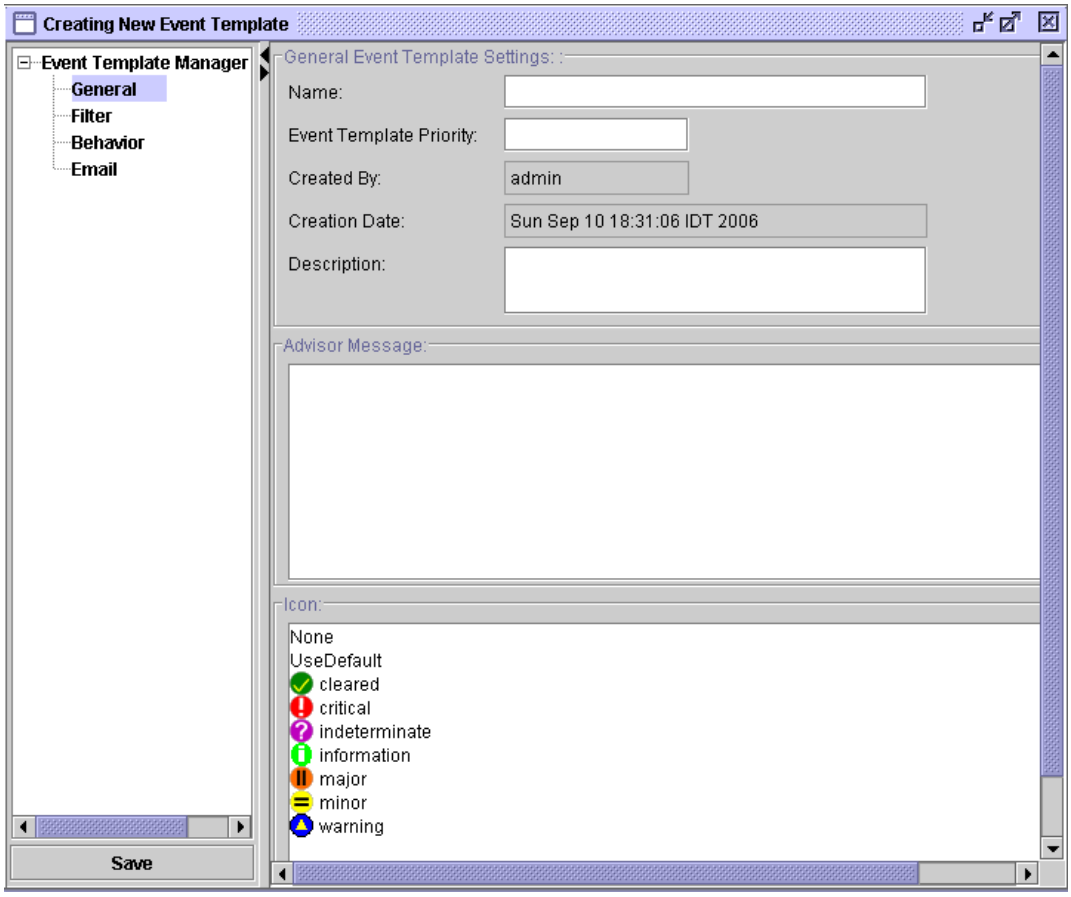

Figure 6-6: Creating New Event Template

The Creating New Event Template window comprises the following main pages:

- ◇ "General Page" on page 184
- ◇ "Filter Page" on page 186
- ◇ "Behavior Page" on page 191
- ◇ "Email Page" on page 194

2 Enter the relevant information in each of the pages.

3 Click the **Save** button to confirm your choices and save them to the database.

6.5.1.1 General Page

In the General page, you can add general information on the template, add a message that will appear in alarms when the template acts, and assign an icon for the template.

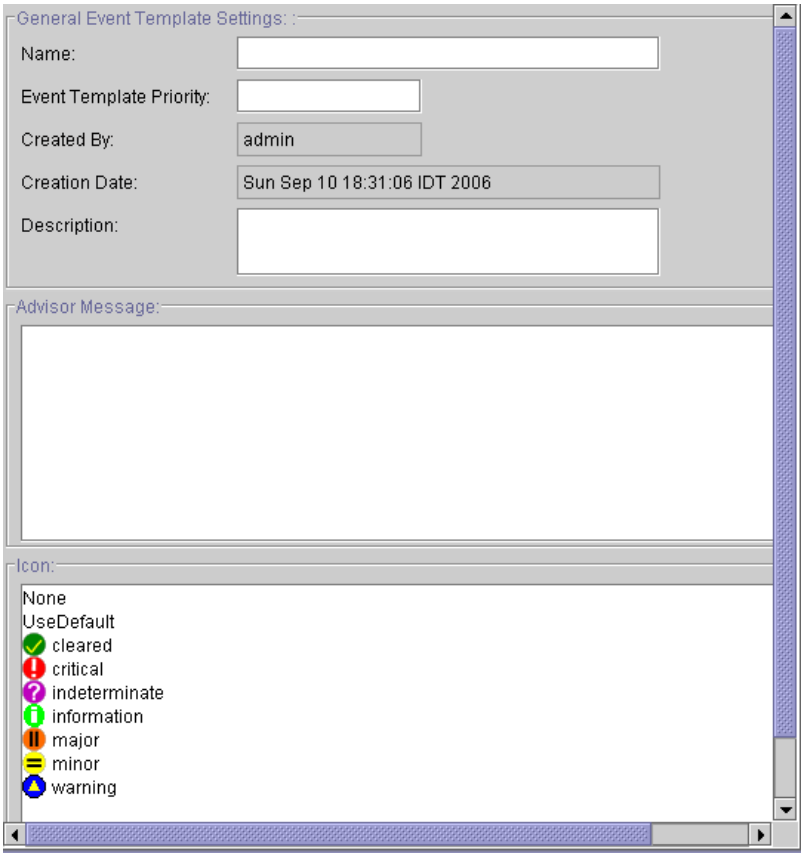

Figure 6-7: Event Template Manager - General Page

The General page comprises the following fields and functions:

Parameter	Description
General Event Template Settings	
Name	The name of the event template.
Event Template Priority	A numerical ranking for this template. The template priority field determines which template processes an alarm if the alarm matches more than one template. The smaller the number defining a template's priority, the higher the priority the template is. The range is: 0~999999.
Created By	A read only display of the user who created the template.
Creation Date	A read only display of the creation date of the template.
Description	An optional description of the template's purpose.
Advisor Message	The message that will appear in alarms when the template acts. The default message comes from the trap's MIB.

Parameter	Description	
Icon	The icon appears in the Alarm display of the Alarm Table, and provides an immediate visual indication of the nature and severity of the alarm. Click to select. The available icons are:	
	None	No icon
	UseDefault	The default icon for the alarm
		Cleared
		Critical
		Indeterminate
		Information
		Major
		Minor
		Warning

6.5.1.2 Filter Page

The Filter page lets you edit Filter Criteria and Protocol Criteria Settings. This filter information matches, or finds, an event template for each alarm received by Event Services. The first template that matches the received alarm controls the processing of that alarm.

Event Services's fault processing logic uses the filtering information provided in the Event Template, along with the templates' priority, to determine which template to use for a given alarm.

NOTE

The smaller the number defining a template's priority, the higher the priority.

For every alarm received, Event Services scans each template, in order of priority (high to low). Event Services selects the first template that matches on each of the filterable fields for alarm processing.

If a template does not define a field (with either a null or empty value, or set to "All") then Event Services does not use the field in the comparison. Empty or "All" in a filterable template field means that the field matches anything. Therefore, Event Services uses only fields that have non-empty or non-"All" values in any comparison.

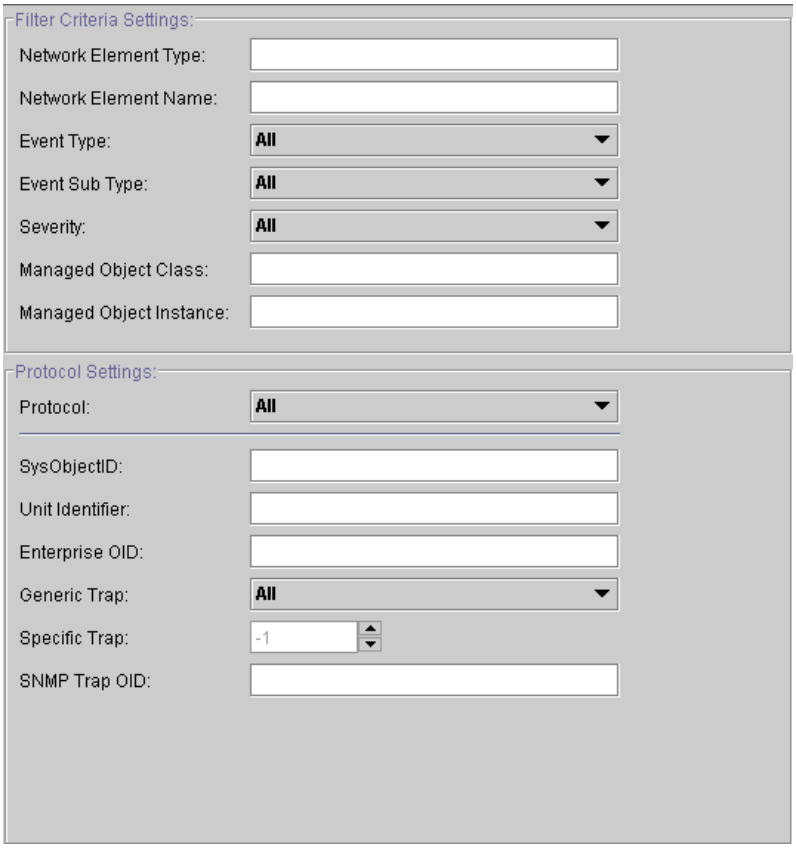

Figure 6-8: Event Template Manager - Filter Page

The Filter page comprises the following fields:

Parameter	Description
Network Element Type	The type of the network element from which the alarm originated.
Network Element Name	The name of the network element from which the alarm originated.
Event Type	Possible values are: All, Alarm, Security Alarm, Informational, Syslog.
Event SubType	Options depend on the selected event type. The default is *All*, but can include *All, Indeterminate, Communications Alarm, Environmental Alarm, Equipment Alarm, Processing Error Alarm, Quality of Service Alarm,* and so on. See Table 6-2.
Severity	The severity of the template's alarm, from *Critical*, *Cleared*, and *All*.
Managed Object Class	The class name of the equipment object where the alarm originated.
Managed Object Instance	The specific instance name of the object where the alarm originated.
Protocol	Options include: *All, Other, SNMPv1, SNMPv2c*, *Q3*, and *Syslog*.

Parameter	Description
Sys ObjectID	The system object ID. Enabled when the protocol is: All, other, Q3.
Unit Identifier	The unit identifier. Enabled when the protocol is: All, other, Q3.
Enterprise OID	The OID assigned to the owning company (enterprise). Enabled when the protocol is SNMPv1.
Generic Trap	A number from 0 to 6 indicating the type of trap. Enabled when the protocol is SNMPv1. The following are valid entries: ■ 0 - Cold Start ■ 1 - Warm Start ■ 2 - Link Down ■ 3 - Link Up ■ 4 - Authentication Failure ■ 5 - Exterior Gateway Protocol (EGP) Neighbor Loss ■ 6 - Use Specific Trap
Specific Trap	The specific trap code as defined in the MIB. Enabled if the Protocol is SNMPv1 and *Generic Trap is* 6 (use specific trap).
SNMP Trap OID	The SNMP trap OID. Enabled if the Protocol is SNMPv2c.

Table 6-1 details the currently supported event filtering information.

Table 6-1: Event Filtering

Event Template GUI Field Name	Description	EventInfo attribute compared with
Network Element Type	Equipment Class for example: com.ngnms.products.vl.common.BWA_VL_AU	ClassName
Network Element Name	Same as RedCell.Config.NetworkResourceIPLookup.Name	NetworkElementName
Event Type	-1:All, 0:Alarm, 1:Security Alarm, 2:Informational, and SysLog	EventType
Event SubType	Further classification of the event. Table 6-2 defines the currently supported sub type values	EventSubType

Table 6-1: Event Filtering

Event Template GUI Field Name	Description	EventInfo attribute compared with
Protocol	Protocol over which the event was received. Table 6-4 defines the currently supported protocol values	EventProtocol
Severity	Severity of the event. Table 6-3 defines the currently supported severity values.	Severity
Managed Object Class	Type of property or resource triggering the event.	ManagedObjectClass
Managed Object Instance	Specific instance of the ManagedObjectClass	ManagedObjectInstance
SysObjectID	SysObjectID	SysObjectID
Unit Identifier	An identifier for the subcomponent of the network element triggering the alarm .	SubComponentID
Enterprise OID	Enterprise Specific OID (SNMPv1 only)	OID
Generic Trap	SNMPv1 Generic Trap Value	Value
Specific Trap	SNMPv1 Specific Trap Value	Specific
SNMP Trap OID	SNMPv2 Trap OID	OID

Table 6-2, Table 6-3, and Table 6-4 detail the currently supported values for the following Event Template Fields: *Event Type*, *Severity*, and *Protocol*.

Table 6-2: Event SubType Value

Event Type	Event SubType[a]	Value[b]
Alarm[c] (0)	Indeterminate	EVENT_SUB_TYPE_INDETERMINATE (1)
	Communications Alarm	EVENT_SUB_TYPE_COMMUNICATIONS_ALARM (2)
	Environmental Alarm	EVENT_SUB_TYPE_ENVIRONMENTAL_ALARM (3)
	Equipment Alarm	EVENT_SUB_TYPE_EQUIPMENT_ALARM (4)

Table 6-2: Event SubType Value

Event Type	Event SubType[a]	Value[b]
	Processing Error Alarm	EVENT_SUB_TYPE_PROCESSING_ERROR_ALARM (10)
	Quality of Service Alarm	EVENT_SUB_TYPE_QUALITY_OF_SERVICE_ALARM (11)
Security Alarm[d] (1)	Indeterminate	EVENT_SUB_TYPE_INDETERMINATE (1)
	Integrity Violation	EVENT_SUB_TYPE_INTEGRITY_VIOLATION (5)
	Operational Violation	EVENT_SUB_TYPE_OPERATIONAL_VIOLATION (8)
	Physical Violation	EVENT_SUB_TYPE_PHYSICAL_VIOLATION (9)
	Security Service or Mechanism Violation	EVENT_SUB_TYPE_SECURITY_SERVICE_OR_MECHANISM_VIOLATION (13)
	Time Domain Violation	EVENT_SUB_TYPE_TIME_DOMAIN_VIOLATION (15)
Informational[e] (2)	Indeterminate	EVENT_SUB_TYPE_INDETERMINATE (1)

a. Refer to the CCITT X.736 and X.733 Recommendations for further information regarding the sub type values.
b. Static final constants for the Event SubType values are defined in the class com.dorado.redcell.assure.fault.IEventInfoConstants
c. Defined by the static final constant com.dorado.redcell.assure.fault.IEventInfoConstants. EVENT_TYPE_ALARM
d. Defined by the static final constant com.dorado.redcell.assure.fault.IEventInfoConstants. EVENT_TYPE_SECURITY
e. Defined by the static final constant com.dorado.redcell.assure.fault.IEventInfoConstants. EVENT_TYPE_INFORMATIONAL

Table 6-3: Event Severity Levels

Severity	Value
Cleared	SEVERITY_CLEARED (0)
Informational	SEVERITY_INFORMATION (1)
Indeterminate	SEVERITY_INDETERMINATE (2)
Warning	SEVERITY_WARNING (3)
Major	SEVERITY_MAJOR (4)
Minor	SEVERITY_MINOR (5)
Critical	SEVERITY_CRITICAL (6)

Table 6-4: Event Protocol Types

Protocol	Value[a]
SNMPv1	EVENT_PROTOCOL_SNMPv1 (“SNMPv1”)
SNMPv2c	EVENT_PROTOCOL_SNMPv2c (“SNMPv2c”)
Q3	EVENT_PROTOCOL_Q3 (“Q3”)
Other	EVENT_PROTOCOL_OTHER (“Other”)

a. Static final constants for the alarm protocol values are defined in the class `com.dorado.redcell.assure.fault.IEventInfoConstants`

6.5.1.3 Behavior Page

The Behavior page provides parameters that determine how Event Services processes matching alarms.

Correlation lets you define two related alarms, and the action to take when a correlated alarm follows an initial alarm. For example, a linkDown alarm, by itself, may call for some corrective action. If it is followed by a linkUp alarm, however, no action is required and the alarm can be cleared.

You can apply thresholds to templates to control when Event Services processes a matching alarm. You can specify a threshold based on the number of matching alarms and duration.

Using thresholds suppresses the display of alarms with a status of Suppressed until the number of alarms of that type exceeds a predetermined number.

NOTE

The correlation rule functionality is intended for the use of Alvarion's development group only.

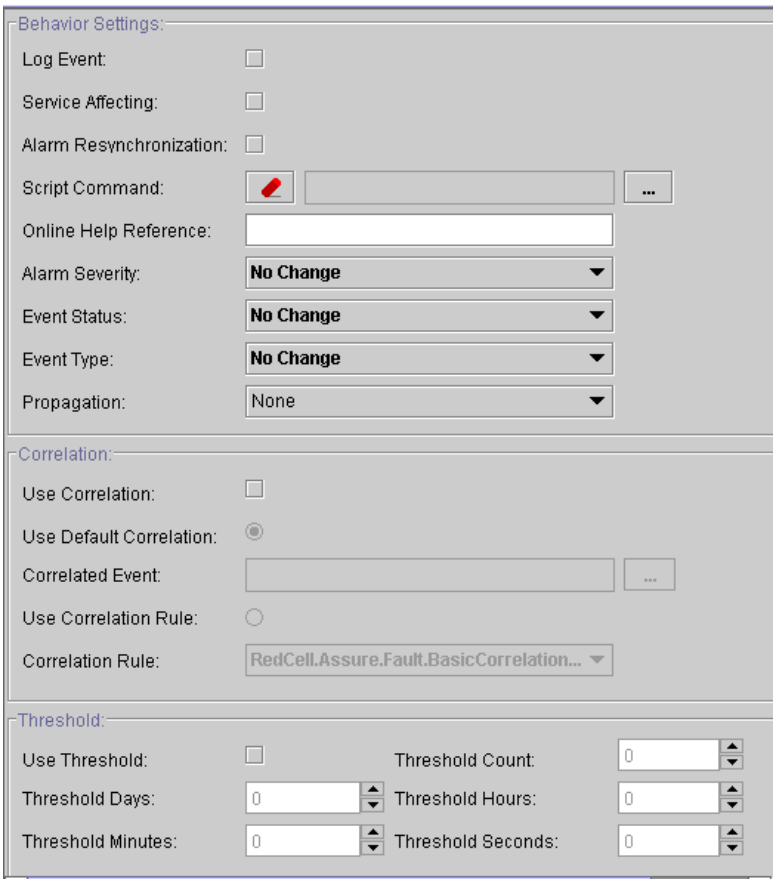

Figure 6-9: Event Template Manager - Behavior Page

The Behavior page contains the following parameters:

Parameter	Description
Behavior Settings	
Log Event	Besides saving each alarm to the database, Event Services can also write the alarm information to a flat file by enabling this option. Enabling this (checking the box) means event services writes all alarms that match this template to a flat file. Log file settings are specified in System Settings.
Service Affecting	This controls whether the alarm should be marked as service affecting or impacting (link down, for example). This affects alarm behavior only for optionally installed Service Level monitoring.
Alarm Resynchronization	This option triggers resynchronization of alarm counts between the network element and the objects in the application's database, when the application receives this alarm.
Script Command	Initiates an external script. Browse for the script command name by clicking the command (...) button. When you click this button, the Command Selector is displayed. See Section 6.9 for information about how to add commands to this selector. Click the eraser icon to remove selected scripts from this field.
Online Help Reference	Currently, this field is informational only. Here, you can store a reference to documentation that may give more detail to the specifics of the actual alarm. For example: this could be a URL.
Alarm Severity	This field modifies the severity level of the alarm. Once Event Services selects the template, before actually processing the alarm, this field overrides the severity of the alarm as it was received from mediation. No change occurs if you set this field to –1 (no change). Refer to Table 6-3 for other valid values.
Event Status	This field modifies the status of the alarm. Once Event Services selects the template, and before actually processing of the alarm, this field overrides the status of the alarm as it was received from mediation. This field will not be used if it is set to a negative one (-1).
Event Type	This field modifies the event type. Once Event Services selects the template, before actually processing the alarm, this field overrides the event type as it was received from mediation. This field will not be used if it is set to a negative one (-1). Refer to Table 6-2 and relevant footnotes for the valid event type values.
Correlation	
Use Correlation	Defines the correlation between two Event Templates. Check to enable.
Use Default Correlation	Check to enable default correlation and browse to select a correlated event template. Alternatively, select the Use Correlation Rule.

Parameter	Description
Use Correlation Rule	Check to enable using a correlation rule and select from the list of available correlation rules.
Threshold	
Use Threshold	Enables thresholding. The remaining settings in this section are only available when *Use Threshold* is selected.
Threshold Count	Specifies the number of alarms the application must receive before it generates an alarm. Use the up and down arrows to change this setting, or enter a number directly.
Threshold Time	The period in hours, minutes, and seconds within which the Threshold Count applies. The number of alarms must exceed what you specify in the Threshold Count within this time window for Suppressed alarms to appear.

Use the up and down arrows to change these settings, or enter the time directly into the Threshold Days, Hours, Minutes, and Seconds.

If you do specify a threshold (and its time parameters), Event Services processes an alarm if the number of alarms received within the threshold time exceeds or equals the threshold count. You can enter any number of days and/or hours and/or minutes and/or seconds. These are treated as the Threshold Duration. For example if the threshold count is 5 and duration if 60 seconds, then Event Services must receive 5 alarms within 60 seconds. Event Services processes only the fifth alarm.

6.5.1.4 Email Page

Use the Email page to enter a message that appears in e-mails when the template acts. You can also enter a subject for the message. Either enter a destination e-mail address from the list. This presupposes e-mail functions within the environment where your host is installed.

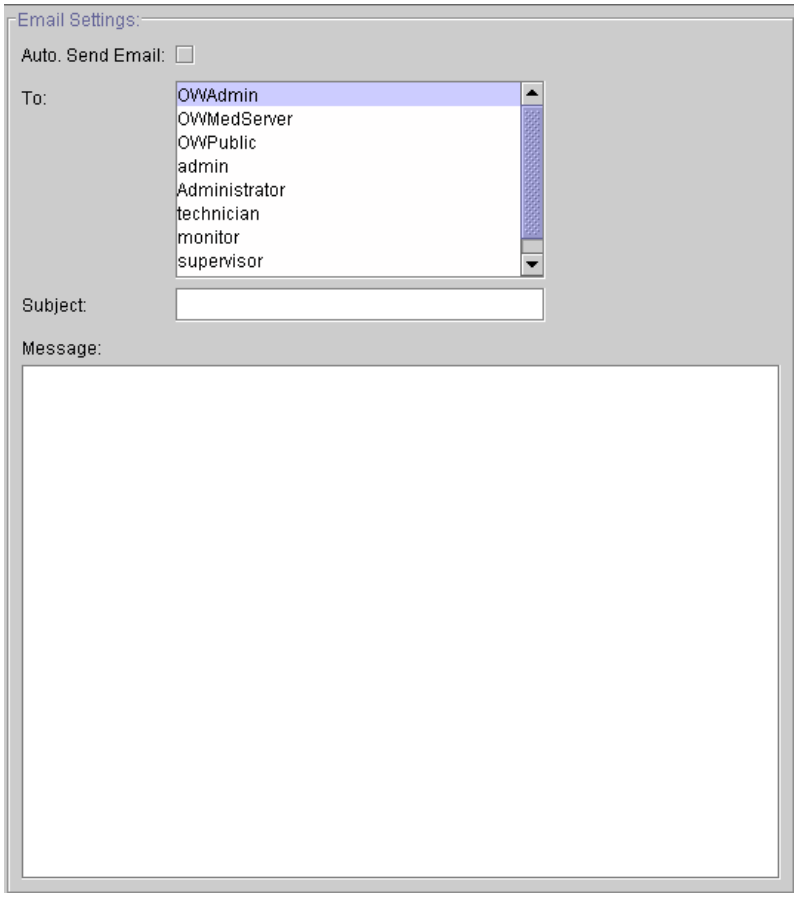

Figure 6-10: Event Template Editor - Email

The fields on the Email panel are:

Parameter	Description
Auto. Send Email	This option sends an e-mail message, as defined in this panel, to the specified recipient whenever the associated alarm occurs.
To	Select the recipient for this e-mail message from the list.
Subject	The subject line of the e-mail message. The default text for this field comes from the Event Description field on the Information panel. Edit it as desired.
Message	The text of e-mail message. The default text comes from the Advisor Message on the Advisor panel. Edit it as desired.

6.5.2 Editing Event Templates

To edit an existing event template:

1 From the Event Template Manager, select an existing template from the list and click **Open**. The Editing Event Template window is displayed:

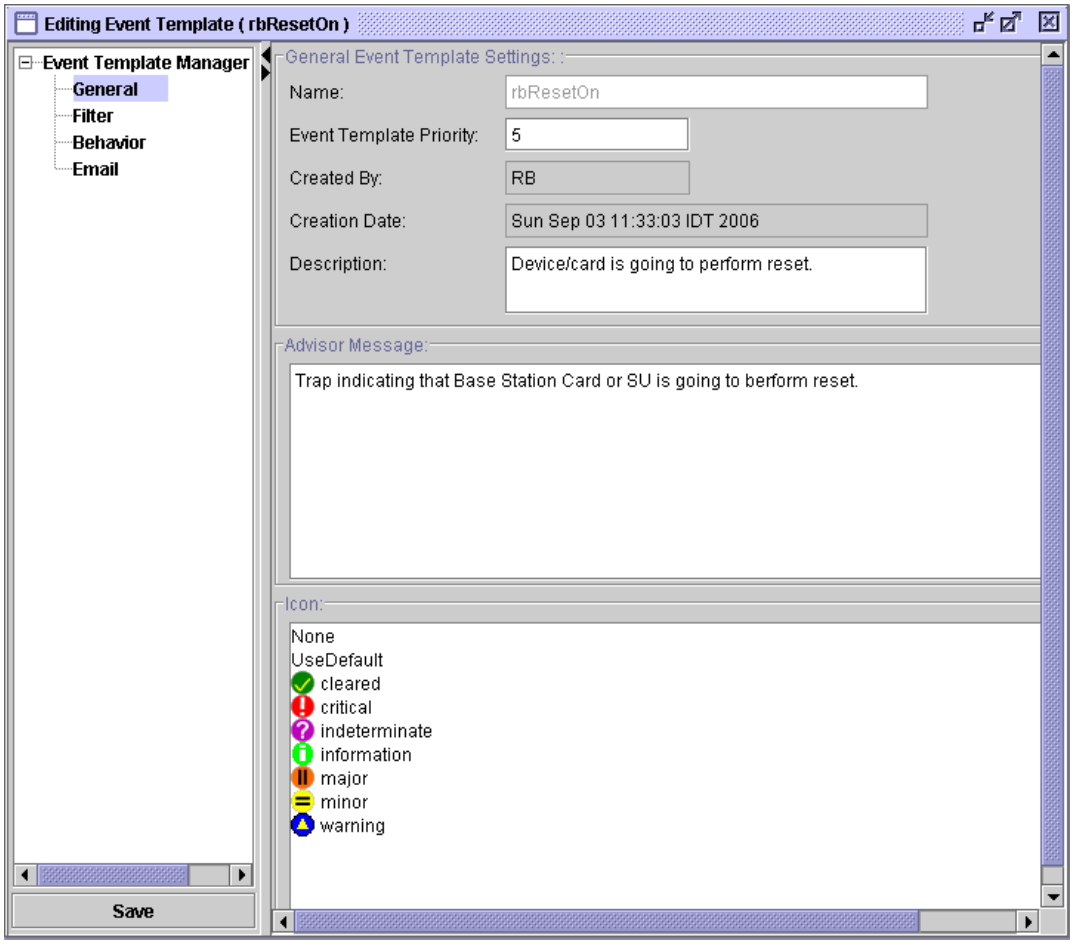

Figure 6-11: Editing Event Template

The Editing Event Template window comprises the following main pages:

- "General Page" on page 184
- "Filter Page" on page 186
- "Behavior Page" on page 191

◇ “Email Page” on page 194

2 Edit the parameters in each of the pages as required.

3 Click **Save** to confirm your choices and save them to the database.

6.5.3 Deleting Event Templates

To delete an Event Template:

1 In the Event Template Manager, select the template to remove and click **Delete**. A confirmation message is displayed.

2 Click **Yes** to confirm the deletion.

6.5.4 Importing Event Templates

You can use the Import utility on templates you create. Exported files can serve as backups or as seed files, and clients running on other servers can import them.

To import an Event Template:

1 Select *Import* from the *File* menu. The *Specify Event Template Manager File to be Imported* window opens.

2 Browse to the template’s location and click **OK**. An *Import Complete* confirmation message appears.

3 Click **OK** to close the confirmation message.

6.6 Northbound Manager

The Northbound Manager provides an interface where you can connect to other management systems, and effectively forward traps. Event Services uses these definitions to enable it to forward notifications to those systems.

Northbound systems include any EMS system (a system receiving information from Event Services), for example: Billing Management Systems, Support Management Systems, Network Management Systems, and Customer Service Systems.

To open the Northbound Manager window:

Select *Event Services* > *Northbound Manager from* the *File* > *Open* menu or from the Navigation Pane.

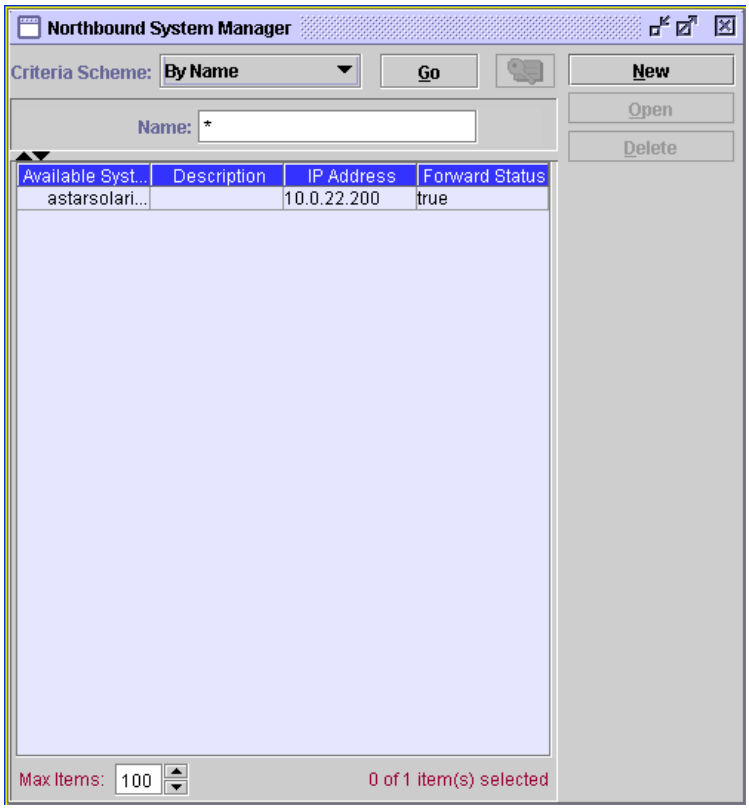

Figure 6-12: Northbound System Manager

The Northbound Manager displays a list of all available systems and provides a description for each. The following are the controls on this manager:

Parameter	Description
New	Creates a new northbound system definition. See Section 6.6.1 for more information.
Edit	Opens an existing northbound system definition for modification. See Section 6.6.1 for more information.
Delete	Deletes a northbound system definition. Select the definition to remove and click **Delete** to delete it.

Associated with the configured northbound system are one or more filters linked with a schedule for when they are active. If a fault matches the criteria of an active filter, then the application forwards it to that destination.

To forward traps:

1. Create at least one forwarding filter that designates what kind of alarms you want to forward. See Section 6.6.3 for more information.
2. Create a new northbound system definition (Section 6.6.1).
3. Assign the filtering you want to this definition.
4. Click the **Start Forwarding** button in the Filter Editor.

6.6.1 Creating or Northbound System Definitions

A northbound system definition, created in the Northbound Manager, tells the application how to communicate with the northbound system, what notifications to send (trap forwarding), and when to send the notifications. It contains the location of the system, associated filters, and Time of Day schedules for the associated filters.

To create/edit northbound system definitions:

1. Click on **New** to create a new definition, or select an existing northbound definition from the list and click on **Open**. The Northbound System Editor, shown in Figure 6-13, is displayed.

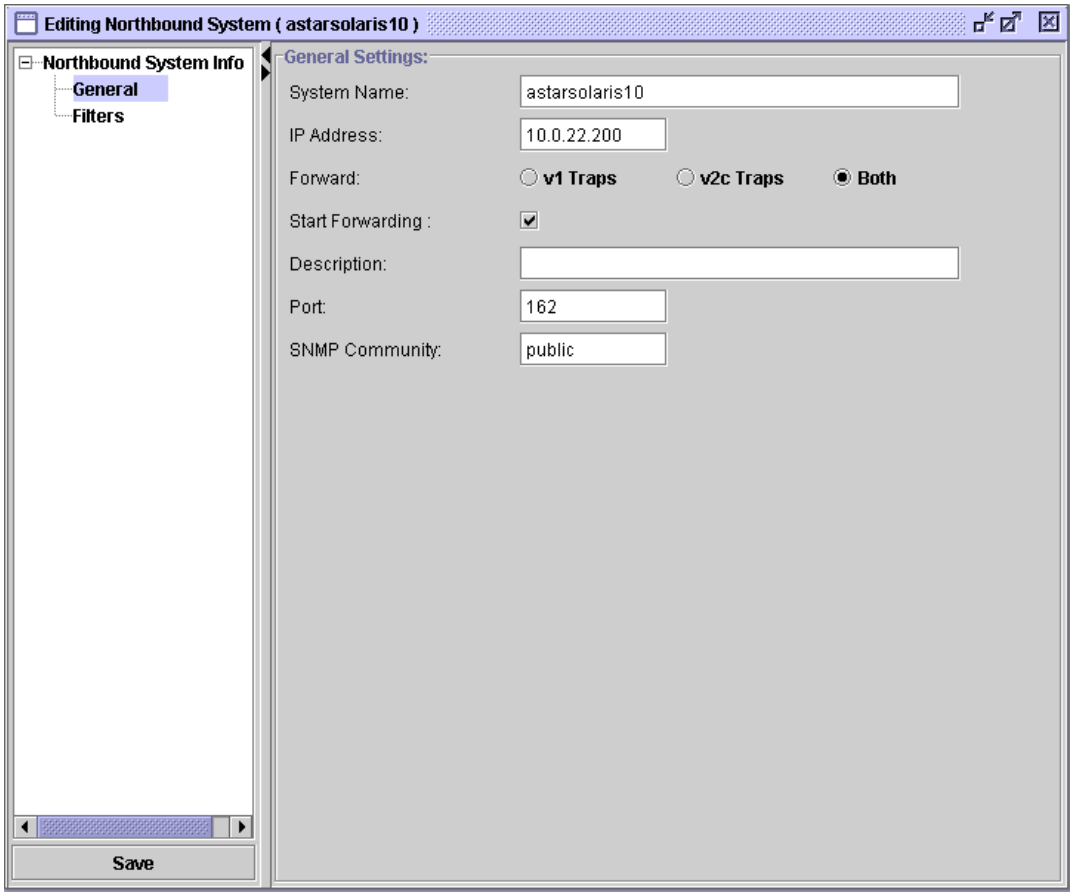

Figure 6-13: Northbound System Editor

The Northbound System Editor window is divided into two main pages:

- General - contains general system information (see Section 6.6.2).
- Filter - contains a list of selected filter settings and their schedule and enables associating new filters with the selected northbound system. See Section 6.6.3 for more about creating and editing filters.

2 Define instances of systems active on the network (see Section 6.6.2).

3 Associate a filter with a northbound system (see Section 6.6.3).

6.6.2 General Page

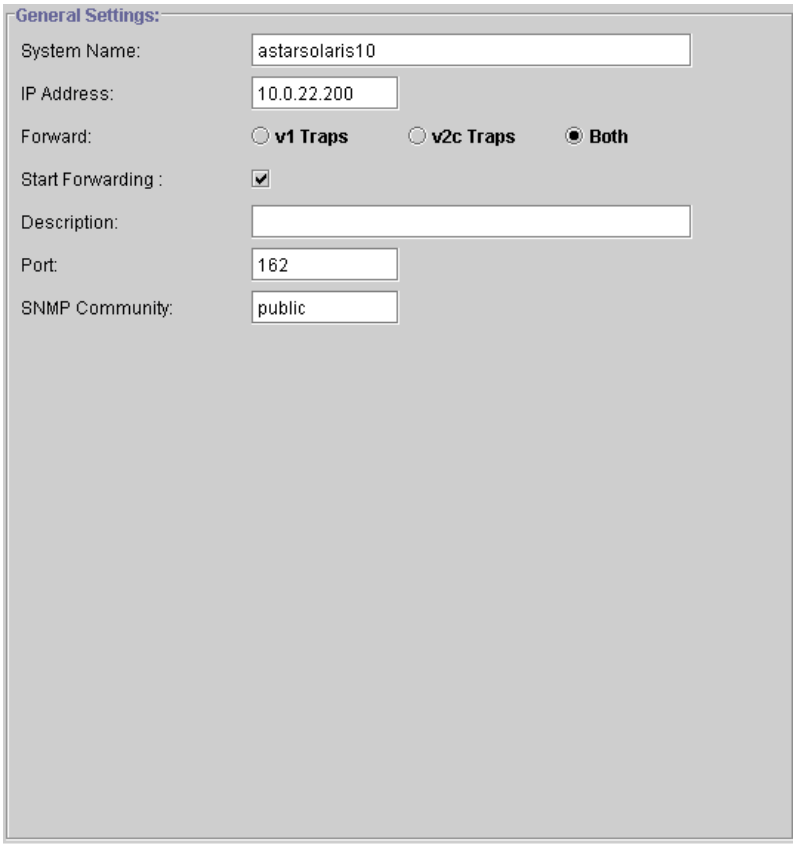

Figure 6-14: Northbound Editor - General Page

The General page contains general system information and includes the following controls and parameters:

Parameter	Description
System Name	The name of the system.
IP Address	The IP address of the host on which the system runs.
Forward	Enables to select whether to forward only SNMP v1 traps, v2c traps, or both.
Start Forwarding	Starts and stops forwarding of alarm reports to the system. You must select this checkbox after having set up northbound system forwarding to begin forwarding traps.
Description	An optional description of the system.
Port	The port number to use to communicate with the system.

Parameter	Description
SNMP Community	The SNMP read-write community of the system.

NOTE

The port configured in the Northbound System editor must match the port your system uses to communicate. Typically, SNMP devices use port 161 to receive set/get requests and port 162 to receive traps. So, typically you must configure Event Services to forward traps to a northbound system with a destination port of 162

6.6.3 Filters Page

From the Filters page you can select filters to associate with the northbound system and schedule their activation only during specific periods.

If you do not add a schedule to a filter, the filter will be always on.

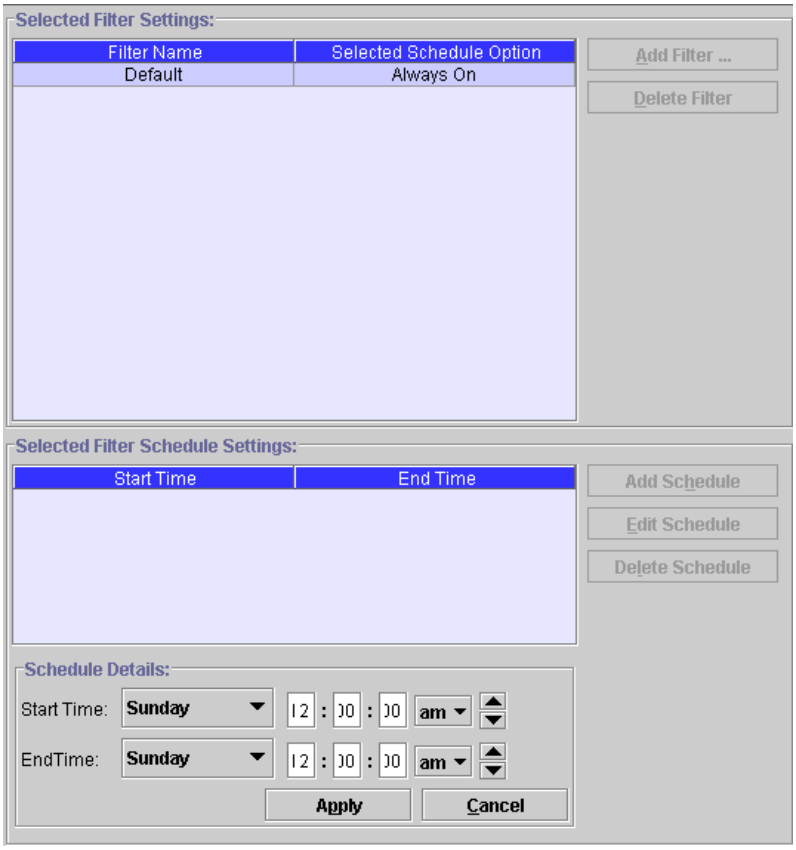

Figure 6-15: Northbound Editor - Filters Page

To associate a filter with a northbound system:

1 In the *Selected Filter Settings* area, click on **Add Filter**. The *Select Event Filter* window opens (see Section 6.8 for details on Event Filters).

2 Select a filter from the list and click **Select**.

Or

Click **New** to create a new filter (see Section 6.8.4 for details on creating Event Filters). After setting all the parameters of the new filter, click **Save** to save and associate the filter with the northbound system.

The selected filters are listed in the *Selected Filter Settings* area.

3 Click **Save** (or Ctrl+S) to save your edits and close the editor, or continue to set a schedule for the filter.

NOTE

You can associate multiple filters with a single northbound system.

To delete the association between a northbound system and a filter:

1 Select a filter from the *Selected Filter Settings* area.

2 Click on **Delete Filter**. The filter is removed from the *Selected Filter Settings* area.

3 Click **Save** (or Ctrl+S) to save your edits and close the editor.

NOTE

The **Delete Filter** function only deletes the association between the northbound system and the filter. The filter still exists in the Event Filter Manager and you can associate it with other system definitions. To delete a filter from the database, see Section 6.8.6.

To schedule the operation of a selected filter:

1 Select a filter in the *Selected Filter Settings* area.

2 In the *Selected Filter Schedule Settings* area, click on **Add Schedule**. The *Schedule Details* area activates.

3 Set the Start Time and End Time.

NOTE

The Start Time and End Time must not be identical.

4 Click **Apply** to add the new schedule to the list of schedules in the *Selected Filter Schedule Settings* area.

NOTE

You can add multiple start and end times to a single filter.

5 Click **Save** (or Ctrl+S) to save your edits and close the editor.

To edit a schedule:

1 With the filter selected, select the schedule to be edited and click on **Edit Schedule**. The *Schedule Details* area activates.

2 Change the settings as required and click **Save** (or Ctrl+S) to save your edits and close the editor.

To remove a schedule:

1 With the filter selected, select the schedule to be deleted and click on **Delete Schedule**. The schedule is removed from the list.

2 Click **Save** (or Ctrl+S) to save your edits and close the editor.

6.6.4 Editing Northbound System Definitions

To edit northbound system definitions:

1 In the Northbound Manager, select an existing northbound definition from the list and click on **Open**. The Editing Northbound System window is displayed.

2 Edit the parameters as required.

3 Click **Save** to confirm your changes and save them to the database.

6.6.5 Deleting Northbound System Definitions

To edit northbound system definitions:

1 In the Northbound Manager, select an existing northbound definition from the list and click on **Delete**. A confirmation message appears.

2 Click **Yes** to confirm the deletion.

6.7 Event View Manager

The Event View Manager lets you create, edit and delete views. When using pre-defined views, specific parameters are shown as configured, allowing you to control alarms more efficiently.

To open the Event View Manager:

Select *Event Services* > *Event View Manager* from the *File* > *Open* menu or from the Navigation Pane. The Event View Manager window is displayed:

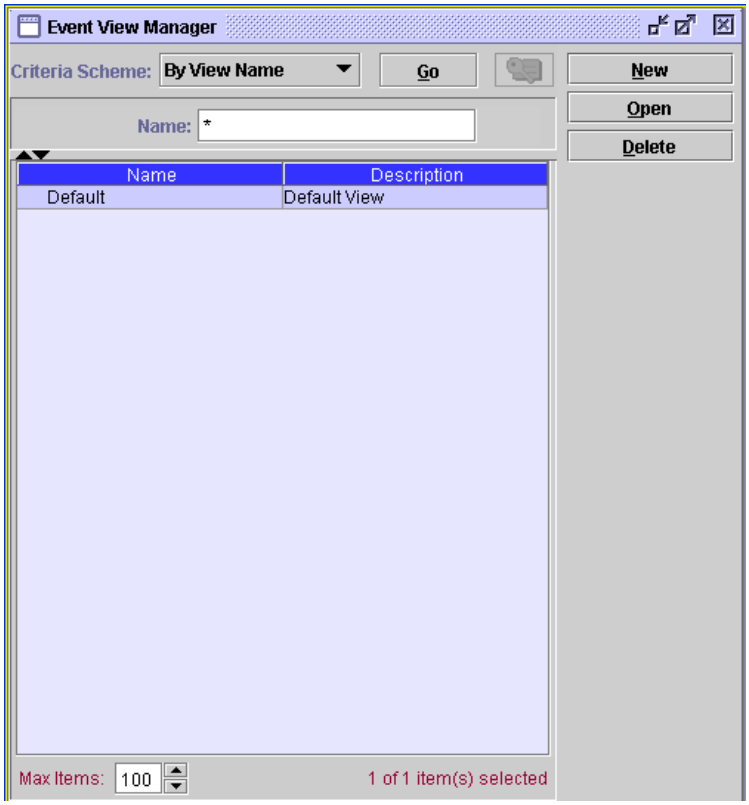

Figure 6-16: Event View Manager

NOTE

You cannot apply a view to an Alarm Table from the Event View Manager. To apply a view, use the View drop-down menu located below the Alarm Table in Event Monitor / Event History window (in the Table Filter & View area).

The following are the controls in the Event View Manager:

Parameter	Description
New	Creates a new Event View. See Section 6.7.3 for more information.
Open	Opens a selected Event View to view/edit its properties. See Section 6.7.4 for more information.
Delete	Deletes selected Event View(s). See Section 6.7.5 for more information.

6.7.1 Filtering Event Views

By default, the Event View Manager displays a list of all defined views. You can filter the list by view name using standard boolean conventions and clicking on **Go**. The new display will reflect all views with the requested string.

You can also limit the number of displayed event views by changing the number in the Max Items box at the bottom left corner and clicking on **Go**.

6.7.2 Default Event View

AlvariSTAR automatically applies the *Default* view to the Event Monitor/Event History's Alarm Tables the first time the Event Monitor/Event History window opens. The default view displays ten alarm attributes: *Equipment Name, Equipment Type, Equipment Location, Event Name, Event Status, Received Time, Ack By, Clear By,* and *Last Update Time* (see Section 6.4.1 for details on all available attributes).

6.7.3 Creating Event Views

To create a new event view:

1 In the Event View Manager, click **New**. The *Creating New Event View* window opens.

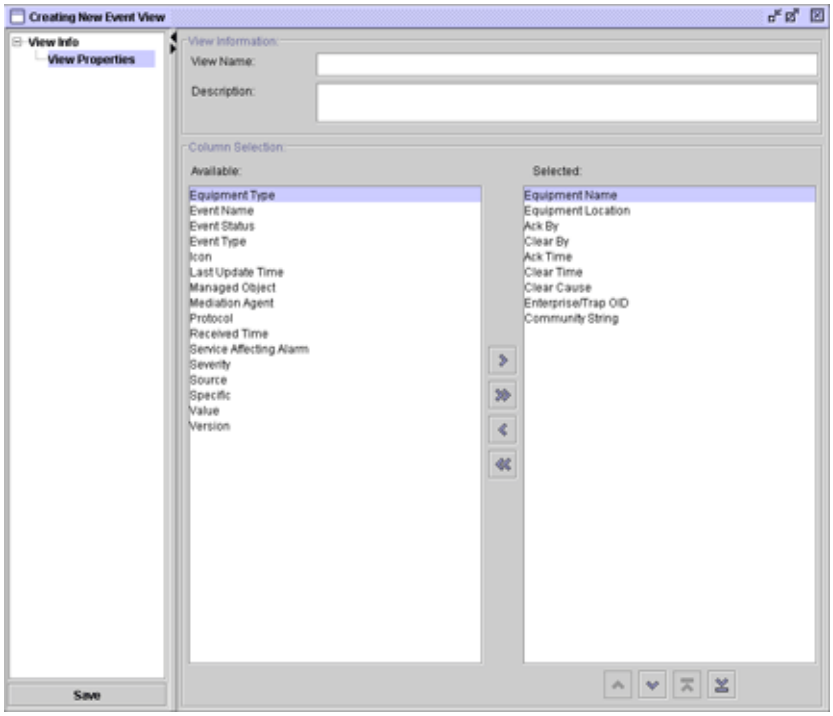

Figure 6-17: Creating New Event View

2 In the View Name field, enter a unique name for the view.

3 Enter a description of the view's use in the Description field (optional).

4 Select the columns that will appear in the Alarm Table by moving items from the Available list to the Selected List. See Section 6.4.1 for information on the available columns. The columns display in Event Monitor/Event History Alarm Tables from left to right according to the order of the items in the Selected list box.

To move items between lists:

To move a single item, select it and click the > or < button. To move several items, hold down the Ctrl key while clicking on the desired items. Click the > or < buttons. To move all items at once, click the >> or << button.

To change the order of the items in the Selected list:

Select the item whose position in the list you want to change and use any of the following controls:

Control	Description
	Moves the item one step up.
	Move the item one step down.
	Moves the selected item to the top of the list.
	Moves the selected item to the bottom of the list.

5 Click **Save** to save the new view and display it in the list of views in the View Manager.

6.7.4 Editing Event Views

To edit an existing event view:

1 In the Event View Manager, select a view from the list.

2 Click **Open**. The *Editing Event View* window opens.

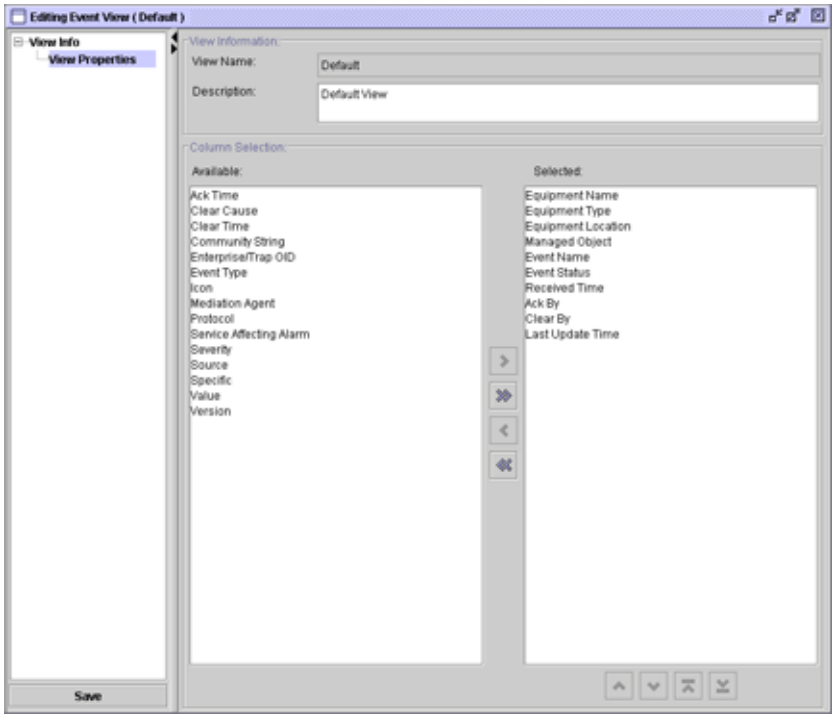

Figure 6-18: Editing Event View

3 Add attributes to the Selected list or remove attributes from the list (see Section 6.7.3 for information on moving items between lists). You can also modify the Description field. The View Name cannot be edited.

4 Click **Save** to save your changes.

6.7.5 Deleting Event Views

To delete an event view:

1 In the Event View Manager, select an event view from the list.

2 Click on **Delete**. A confirmation window opens.

3 Click **Yes** to confirm the deletion, or **No** to cancel it.

6.8 Event Filter Manager

The Event Filter Manager lets you create, edit and delete filters to the Event Monitor/Event History windows. When using pre-defined filters, specific Alarm types are displayed, allowing you to control alarms more efficiently.

To open the Event Filter Manager:

Select *Event Services* > *Event Filter Manager* from the *File* > *Open* menu or from the Navigation Pane. The Event Filter Manager window is displayed:

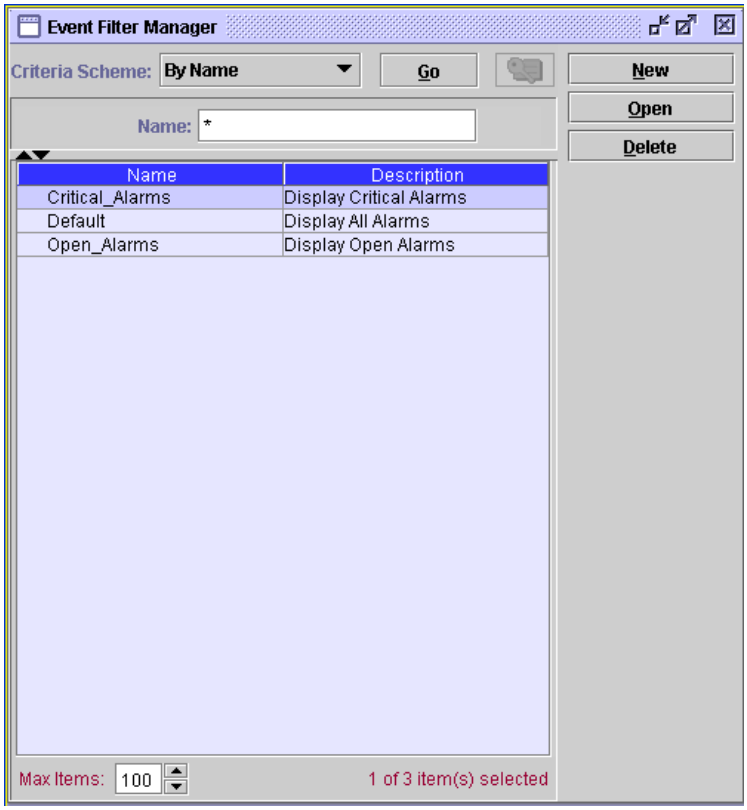

Figure 6-19: Event Filter Manager

NOTE

You cannot apply an event filter to the Alarm Table in the Event Monitor / Event History from the Event Filter Manager. To apply a filter, use the Filter drop-down menu located below the Alarm Table in Event Monitor / Event History window (in the Table Filter & View area).

The following are the controls in the Event Filter Manager:

Parameter	Description
New	Creates a new Event Filter. See Section 6.8.4 for more information.
Open	Opens a selected Event Filter to view/edit its properties. See Section 6.8.5 for more information.
Delete	Deletes selected Event Filter(s). Select the filter(s) to remove and click on **Delete**. The application prompts you for confirmation.

6.8.1 Filtering Event Filters

By default, the Event Filter Manager displays a list of all defined views. You can filter the list by view name using standard boolean conventions and clicking on **Go**. The new display will reflect all views with the requested string.

You can also limit the number of displayed event filters by changing the number in the Max Items box at the bottom left corner and clicking on **Go**.

6.8.2 Default Event Filter

The default filter automatically applies to Event Monitor/Event History's Alarm Tables the first time Event Monitor/Event History opens. The default filter lets all alarms appear in the manager.

6.8.3 Managing Filter Criteria

You can manage Filters by selecting from the available filter criteria. For every criterion, you need to select a Connector, an Attribute (and a value for that attribute), and an Operator. The following are their definitions:

- Connector: Adds a logical connector (Add/Or) to the filter criteria associated with a particular attribute.

- Attribute: Selects an attribute to add to the filter criteria. Filters are based on these attributes. The following are the available attributes:

  - Equipment Contact - the contact(s) associated with the equipment to which the alarm relates
  - Equipment Location - the physical location of the equipment
  - Equipment Name - the name of the equipment
  - Equipment Type - the type of equipment:

- Base Station
- Micro Base Station
- SU
- NPU
- AU

- Event Template Name - the template associated with the alarm
- Event Type:
  - 0 (Alarm)
  - 1 (Security Alarm)
  - 2 (Informational)
  - 3 (Syslog)
  - 4 (EMS Alarm)
- Managed Object Name
- Received Time - filters based on the time that the alarms was received:
  - Relative to Current Time - enables to specify the number of days, hours, and minutes before current time.
  - Specific Time - enables to enter a specific date/time
- Service Affecting - indicates if the alarm affects a service (True/False)
- Severity - the severity of the alarm (see Section 6.4.2 for a detailed description of the available severities):
  - 0 (Cleared)
  - 1 (Informational)
  - 2 (Indeterminate)
  - 3 (Warning)
  - 4 (Minor)
  - 5 (Major)
  - 6 (Critical)
- Source - the IP address of the object or device that sent the alarm

- Status - the status of the alarm:
  - Cleared
  - Informational
  - Open
  - Suppressed

- Operator: allows to define the relationship between the attribute and the selected value. The available operators are:
  - = equals to
  - <> not equals to
  - > greater than
  - < less than
  - >= greater than or equals to
  - <= less than or equals to
  - LIKE Values are case sensitive. LIKE also supports wildcards: *, [], \, and ?. Use **?** to search for single characters, **[]** for multiple characters, and **** as escape to search for special characters. For example, **\?** will search for **?** rather than treating **?** as a wildcard. Use ***** for any string.

- Value - allows to select a specific value to the particular attribute. Allowable values are attribute-specific.

Use the following controls to manage the list of criteria:

Parameter	Description
Add	Adds the defined Connector, Attribute, Operator, and Value to the filter criteria.
Delete	Deletes a selected row of filter criteria. Select the criterion(s) to remove and click on **Delete**.
Delete All	Deletes all the filter criteria. The application prompts you for confirmation.
Not	Adds a NOT logical operator to the row of filter criteria.

Parameter	Description
( )	Adds parentheses to the filter criteria. You can add parentheses around multiple rows of the filter criteria.
Up/down arrows	Changes the position of a row in the filter criteria.
Save	Saves the filter definition.

6.8.4 Creating Event Filters

To create a new event filter:

1 In the Event Filter Manager, click **New**. The *Creating New Event Filter* window opens.

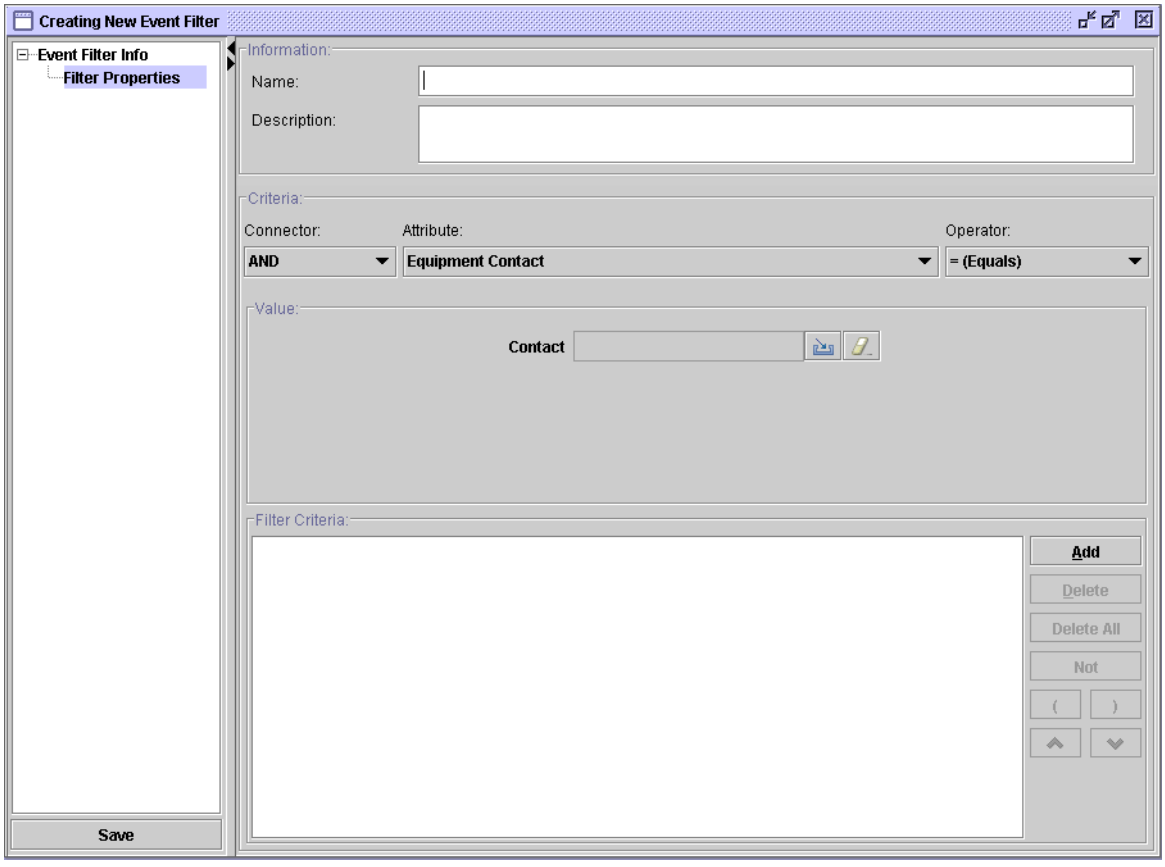

Figure 6-20: Creating New Event Filter

2 In the Name field, enter a unique name for the view.

3 Enter a description of the filter in the Description field (optional).

4 Add the required filter criteria (see Section 6.8.3). As you define the filter criteria, the currently defined options appear in the Filter Criteria area at the bottom of the Event Filter Editor.

5 Click **Save** to save the new filter and display it in the list of filters in the Filter Manager.

6.8.5 Editing Event Filters

To edit an existing event filter:

1 In the Event Filter Manager, select a filter from the list.

2 Click **Open**. The *Editing Event Filter* window opens.

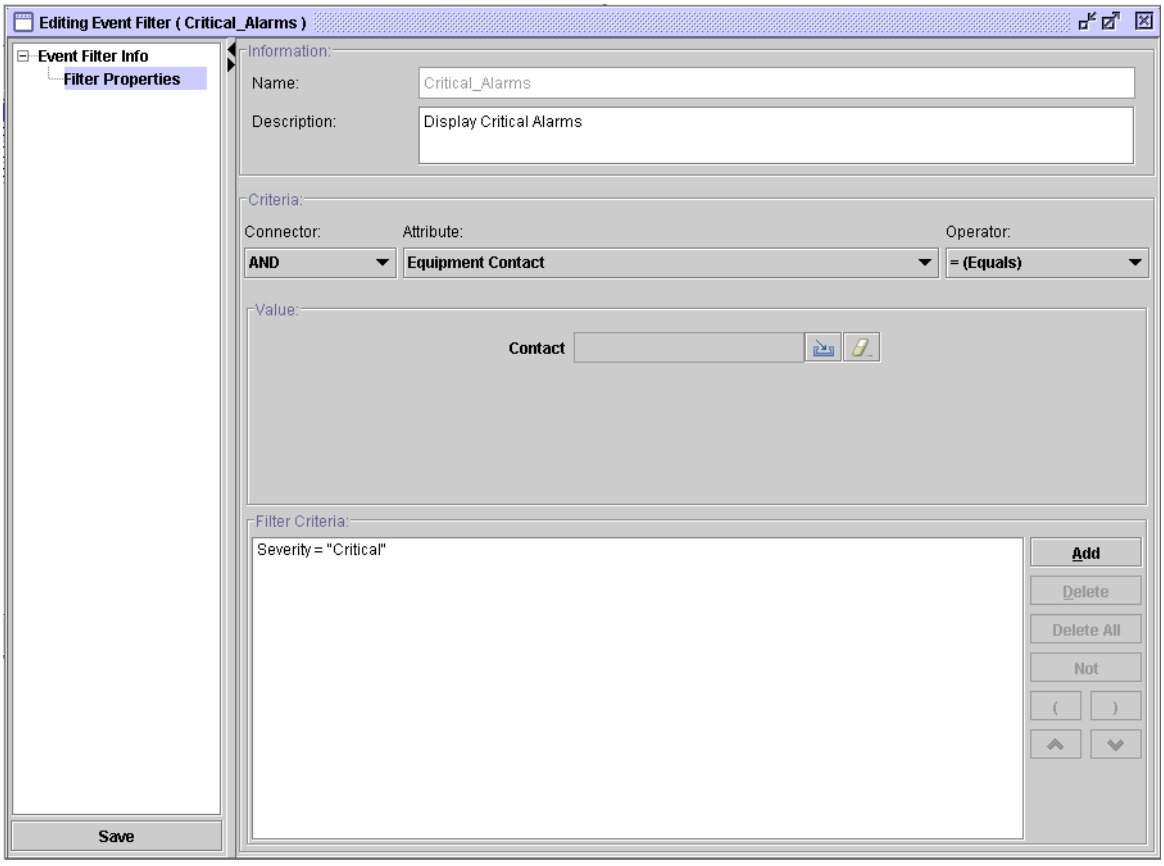

Figure 6-21: Editing Event Filter

3 Edit the required filter criteria (see Section 6.8.3). The filter's Name cannot be changed.

4 Click **Save** to save your changes.

6.8.6 Deleting Event Filters

To delete an event filter:

1 In the Event Filter Manager, select a filter from the list.

2 Click **Delete**. A confirmation window opens.

3 Click **Yes** to confirm the deletion, or **No** to cancel it.

6.8.7 Archiving Alarms

To ensure your database does not fill up with alarms, you can archive them via the Database Aging task. See Section 5.2.4 for further details.

6.9 Command Manager

Template-matched alarms can trigger external scripts. These script commands can even have parameters that come from values in the *EventInfo* alarm's attributes, or other assigned constants. The manager lists available script commands. You can create, edit and delete script commands with the buttons on this manager.

To open the Command Manager:

Select *Event Services* > *Command Manager* from the *File* > *Open* menu or from the Navigation Pane. The Command Manager window is displayed:

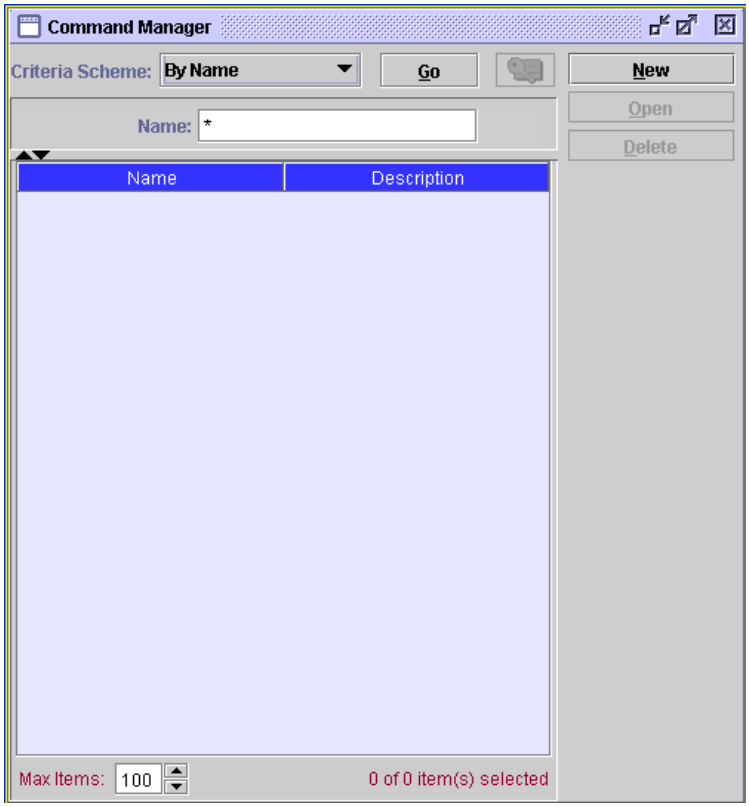

Figure 6-22: Command Manager

The Command Manager displays a list of all available commands and provides a description for each.

From the Command Manager, you can:

- Create new commands - Section 6.9.1
- Modify existing commands - Section 6.9.2
- Delete commands - Section 6.9.3

6.9.1 Creating Commands

To create new commands:

1 From the Command Manager, click **New** to define a new command. The Creating New Command window is displayed:

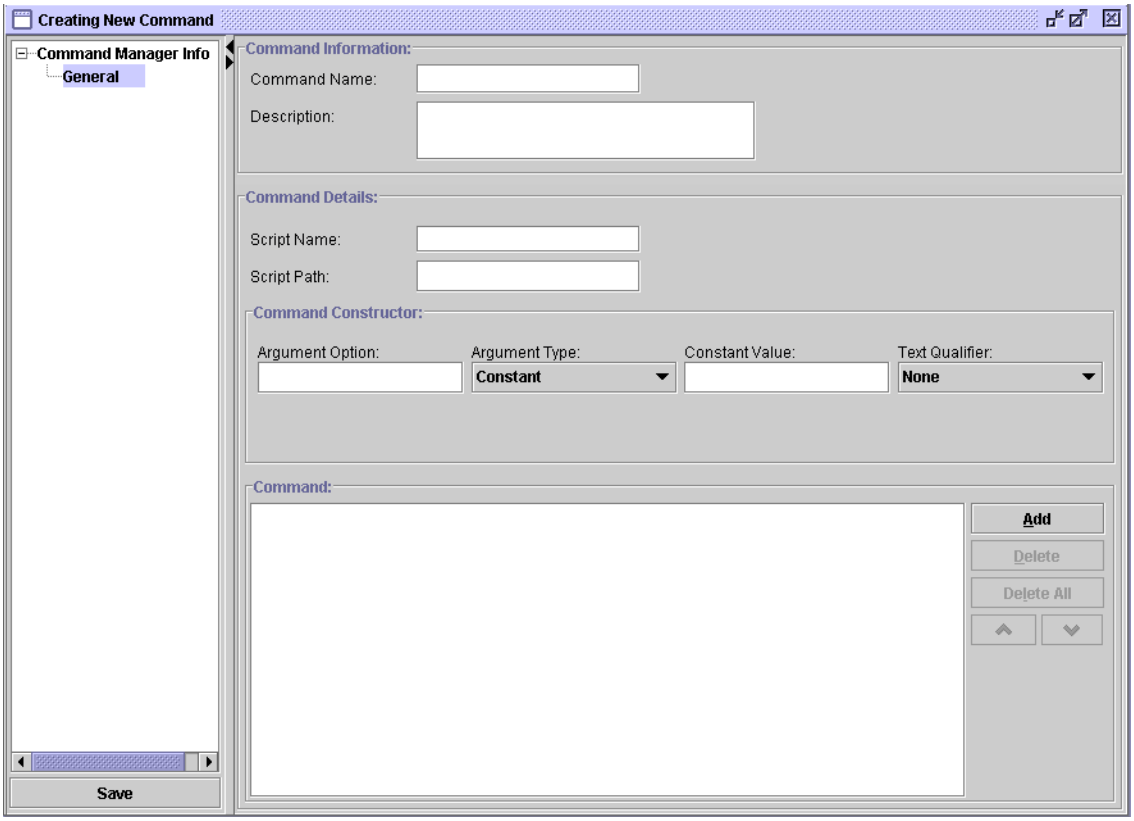

Figure 6-23: Creating New Command

You can configure your script with the following fields:

Parameter	Description
Command Name	A unique text identifier.
Description	A text description
Script Name	The name of the script to run
Script Path	The location of the script. Describe either a Windows or UNIX path.
Command Constructor	Enter parameters to append to the selected script here. The *Argument Option* can be something like -a. The *Argument Type* drop list lets you select either a constant or an EventInfo attribute. If you select a constant, the next field is *Constant Value* (a text field). If you select EventInfo attribute, the next field is a drop list of the attributes available. The final field is *Text Qualifier* which lets you select whether this parameter needs double, single quotes, or no qualifier. When you select quotes, the parameter looks like this: -a “surrounded by quotes”.
Command	This section of the screen displays the script command as you assemble it. Click the **Add** button on the right to assemble the complete script command. Added parameters always appear last on the list in this area, but you can use the arrow keys to re-arrange their order, and the *Delete* button to remove parameters (but not the script). *Delete All* removes everything.

2 Click the **Add** button to assemble the complete script command. Added parameters always appear last on the list, but you can use the arrow keys to re-arrange their order, or use the **Delete** button to remove parameters (not the script). **Delete All** removes everything.

3 Click **Save** to add your command script to the list of available scripts.

6.9.2 Editing Commands

To edit a command:

1 From the Command Manager, select an existing command from the list and click **Open**. The Editing Command window is displayed.

2 Edit the parameters in each of the pages as required. The name of the command cannot be edited.

3 Click **Save** to confirm your choices and save them to the database.

6.9.3 Deleting Commands

To delete a Command:

1. In the Command Manager, select the command to remove and click **Delete**. A confirmation message is displayed. You can select several commands using the Ctrl key.
2. Click **Yes** to confirm the deletion.

Index

A

Abort task 5-129
About AlvariSTAR 1-2
About Window 1-14
Accelerators 1-24
Accounts, disabled 1-12
Activating Licenses 5-158
Active Alarms
  Control Buttons 6-180
Add
  Licenses 5-158
  Service Profile 4-98
Add task 5-129
Alarm Details Window 6-175
  Event Detail Page 6-176
  Opening 6-175
Alarm Management 6-179
Alarm Severities 6-174
Alarm Severity & Count
  Event History 6-170
  Event Monitor 6-167
Alarm Table 6-172
  Event History 6-171
  Event Monitor 6-168
  Limiting the number of alarms 6-173
Alarms
  archiving 6-217
  Limiting the number of alarms 6-173
Allow Password Reuse 2-53
Allow UserId in Password 2-53
AlvariSTAR
  Exit 1-10
  Shut down the client 1-10
  Version number 1-14
AlvariSTAR, starting 1-9
Application Security Policy 2-48
Application Server 1-13
Archiving Alarms 6-217
Associating a filter with a northbound system 6-203
Audit Log Manager 5-161
  Opening 5-161
Audit Logs
  Exporting 5-163

B

Backup Files Manager
  Opening 3-77
Browser View 1-22

C

Cascade the MDI View 1-23
Change Password 1-11
Clear Schedule (of tasks) 5-129
Command Manager 6-218
  Deleting 6-221
Commands
  Creating 6-219
  Deleting 6-221
  Editing 6-220
Configuration Backup Task 5-154
  Open 5-154
Contact Manager
  Associating devices with a contact 3-75
  creating a contact 3-75
  modifying a contact 3-75
  Opening 3-74
Control Buttons 1-24
Conventions 1-24
Creating a contact 3-75
Creating a new Service Profile 4-98

Creating a new Subscriber 4-115
Creating commands 6-219
Creating Event Filters 6-215
Creating Event Templates 6-183
Creating Event Views 6-207
Creating northbound system definitions 6-199
Customizing Views in Event History 6-173
Customizing Views in Event Monitor 6-173

D

Database Aging Task 5-135
  Archiving alarms 6-217
  Edit 5-135
Default Event View 6-207
Default Password 1-9
Default User ID 1-9
Defining
  Locations 3-71
Defining Locations and Sub Locations 3-71
Delete
  Service Profile 4-98
Delete task 5-129
Deleting a Service Profile 4-98
Deleting a Subscriber 4-115
Deleting Commands 6-221
Deleting event Filters 6-217
Deleting Event Templates 6-197
Deleting event Views 6-210
Deleting the association between a northbound system and a filter 6-203
Deploying Service Profiles 4-108
Disabled Accounts 1-12
Displaying the Navigation Pane 1-21

E

Edit
  Database Aging Task 5-135
  Network Scan Task 5-134
  Service Profile 4-98
Edit task 5-129
Editing a Subscriber 4-115
Editing Commands 6-220
Editing Event Filters 6-216
Editing Event Templates 6-196
Editing Event Views 6-209
Equipment Editor
  Opening 3-64
Equipment Manager 3-61
  Delete 3-63
  Multiple Config 3-64
  Opening 3-61
Event Detail Page 6-176
Event Detail Window
  Advisor 6-179
  Notes 6-179
  Variable Binding List 6-178
Event Filter Manager 6-211
  Archiving Alarms 6-217
  Creating event filters 6-215
  Default Event Filter 6-212
  Deleting event filters 6-217
  Editing event filters 6-216
  Filtering Event Filters 6-212
  Opening 6-211
Event Filters
  Creating 6-215
  Deleting 6-217
  Editing 6-216
  Scheduling in a northbound system 6-203
Event History 6-170
  Alarm Severity & Count 6-170
  Alarm Table 6-171
  Last Refresh Time 6-171
  Maximum Rows 6-171
  Table Filter and View 6-171
Event Monitor 6-167
  Alarm Severity & Count 6-167
  AlarmTable 6-168
  Control Buttons 6-168
  Last Refresh Time 6-168
  Listening mode 6-167
  Maximum Rows 6-168
  Opening 6-167
  Refresh Rate 6-168

Table Filter and View 6-168
Event Services 6-166
Alarm Operations menus 6-179
Command manager 6-218
Context menu 6-179
Exporting Alarms 6-180
Event Template Editor
Online help reference 6-193
Event Template Filtering 6-186
Event Template Manager
Alarm resynchronization 6-193
Behavior 6-191
Correlation settings 6-192
Creating Event Templates 6-183
Deleting 6-197
Editing 6-196
Email 6-194
Filter 6-186
General 6-184
Log event 6-193
Service affecting 6-193
Threshold 6-194
Threshold Settings 6-192
Event View Manager 6-206
Creating event views 6-207
Default Event View 6-207
Deleting event views 6-210
Editing event views 6-209
Filtering Event Views 6-207
Opening 6-206
Event Views
Creating 6-207
Deleting 6-210
Editing 6-209
Exit the application 1-10
Expired Account Age 2-49
Exporting
Audit Logs 5-163
Exporting Alarms 6-180
Exporting performance collection data 3-87

F

Filter and View Table
Event History 6-171
Event Monitor 6-168
Filtering Event Filters 6-212
Filtering Event Views 6-207
Filters 1-26
Functional Permissions 2-43
Associating a new Principal 2-44
Function Associations 2-45
Functions Panel 2-44
Granting Permissions 2-43
Principal Panel 2-44
Functional Permissions Editor 2-45
Functional Permissions Page 2-44
Functions
Associating Functions 2-45
Functions Associations
Modifying Function Associations 2-45
Removing Function Associations 2-45

G

Graph Generator 3-83
Group Assignments
Adding 2-38
Removing 2-38
Group Editor 2-41
Group Rights Summary 2-54

H

Help Navigator window 1-28
Help Topic 1-28
Hiding the Navigation Pane 1-21
Home Window 1-14

I

Idle Account Age 2-49
Importing
Event templates 6-197

L

Last Refresh Time 6-168
  Event History 6-171
License 1-6
  Activate 5-158
  Add 5-158
License Manager 5-157
  Open 5-157
Limiting the Result Set 1-27
Listening mode 6-167
Location Editor 3-69
  Coordinate Types 3-71
  Creating a location 3-69
  Modifying a location 3-69
Location Manager 3-67
  Opening 3-67
Location Map
  Defining Locations 3-71
Lockout Period 2-49
Logging Off 1-10
Logging On 1-9
Login Attempts 2-50
Login Policy 2-48
  Editing 2-49
  Expired Account Age 2-49
  Idle Account Age 2-49
  Inactivity Timeout 2-49
  Lockout Period 2-49
  Login Attempts 2-50
  Privacy Warning 2-49
Login Policy settings 1-12
Login Policy settings, changing 1-13

M

Main Menu 1-15
Main Window 1-15
Managed Network Application
  Opening 3-56
Maps 1-6
Maximum Rows 6-168
  Event History 6-171
MDI View 1-22
  cascading 1-23
  tile 1-23
Minimum Password Length 2-53
Modify task 5-129
Modifying a Service Profile 4-98

N

Navigation Pane 1-19
  displaying 1-22
  hiding 1-21
  Tree view 1-19
Network IP Address Ranges
  Export button 3-59
  exporting a range 3-59
  Import button 3-59
  Importing a range 3-59
Network Management System (NMS) 1-2
Network Operation Centers (NOCs) 1-2
Network Scan Task 5-134
  Edit 5-134
New task 5-129
NMS (Network Management System) 1-2
NOCs (Network Operation Centers) 1-2
Northbound Manager 6-198
  Associating a filter 6-203
  Creating system definitions 6-199
  Deleting a filter association 6-203
  Deleting system definitions 6-205
  Editing system definitions 6-204
  Forwarding traps 6-199
  Opening 6-198
  scheduling filters 6-203

O

Open
  Audit Log Manager 5-161
  Configuration Backup Task 5-154
  License Manager 5-157
  Performance Collection Task 5-141
  Service Manager 4-91
  Service Profile Manager 4-95

Single Range Scan Task 5-137, 5-138
Software Upgrade Task 5-147
Open task results 5-133
Opening the Subscriber Editor 4-115
Opening the Subscriber Manager 4-113

P

Password
changing 1-11
Policy settings 1-12
Password Constraint 2-52
Allow Password Reuse 2-53
Allow UserId in Password 2-53
Require a number 2-53
Require a special character 2-53
Password Expiration Age 2-51
Password Expiration Warning 2-51
Password History 2-51
Password Policy 2-50
Minimum Password Length 2-53
Password Expiration Age 2-51
Password Expiration Warning 2-51
Password History 2-51
Required Mixed Case 2-53
Passwords
constraints 1-11
Performance Collection
Exporting Data 3-87
Performance Collection Task 5-140
Open 5-141
PM Collection
Graph 3-83
Post Installation Checklist 1-6
Privacy Warning 2-49

Q

Quick Start 1-7

R

Rearranging columns 1-25
Refresh Rate 6-168
Require a number 2-53
Require a special character 2-53
Require Mixed Case 2-53
Resizing columns 1-25
Run task 5-129

S

Scheduling filters 6-203
Scheduling tasks 5-130
Scripts 6-218
Security Enforcement 1-7
Service Manager 4-91
Associated Subscriber 4-93
Open 4-91
Performance Monitoring 4-94
Service Profile Distribution Task 4-108, 5-137
Service Profile Editor 4-98
Deploying service profiles 4-108
managing templates 4-99
Reuse components 4-99
Saving Templates 4-99
Using components from Managed Devices 4-99
Using templates 4-99
Service Profile Manager 4-95
Delete 4-98
Edit 4-98
New 4-98
Open 4-95
Service provisioning 4-90
Shortcuts 1-24
Single Range Scan Task 5-138
Open 5-137, 5-138
Slide Menu View 1-19
SNMP Ports 1-7
Software Upgrade Task 5-146
Open 5-147
Sorting tables 1-25
Status Bar 1-23
Subscriber
Delete 4-115
Edit 4-115
New 4-115

Subscriber Editor 4-116
Open 4-115
Subscriber Manager 4-113
Open 4-113
SW Upgrade Files 1-6

T

Tables
Rearranging columns 1-25
Sorting 1-25
Tables, working with 1-25
Task
Configuration Backup 5-154
Database Aging 5-135
Network Scan 5-134
Performance Collection 5-140
Service Profile Distribution 5-137
Single Range Scan 5-138
Software Upgrade 5-146
Task Manager 5-127
Abort 5-129
Add 5-129
Clear schedule 5-129
Delete 5-129
Edit 5-129
Opening 5-127
Reports 5-130
Run 5-129
Schedule task 5-130
Service profile distribution 4-108
Viewing reports 5-130
Task Results
Opening 5-133
Template Behavior 6-191
Threshold 6-194
Tile the MDI View 1-23
Toolbar 1-17
Traps, forwarding 6-199
Tree View 1-19

U

User Group Manager 2-40
Adding a group 2-41
Default User 2-42
Default User Group 2-42
Deleting a group 2-42
Group Editor 2-41
Modifying a group 2-41
User Manager 2-31
Adding Users 2-33
Controls 2-32
Filtering 2-32
Filtering by group 2-32
General tab 2-34
Groups tab 2-37
Profile tab 2-35
Sorting 2-32
User Monitor 5-159
Current Logged In Users table 5-159
Logged in users 5-159
Opening 5-159
Sending Message window 5-160
Terminating 5-160
User Monitor Window
Current Logged In Users 5-159
Users
Adding 2-33
Disabling 2-32
Modifying 2-33
Unlocking 2-33
Users, logged in 5-159

V

Variable Binding List 6-178
Viewing reports of completed tasks 5-130

W

wildcard characters 1-26
Work Area 1-22